

THÈSE

DE DOCTORAT DE TROISIÈME CYCLE DE MATHÉMATIQUES PURES

présentée

A L'UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE
DE GRENOBLE

par

Marie-Josée FERTON

SUR L'ANNEAU DES ENTIERS D'EXTENSIONS CYCLIQUES

DE DEGRE p ET D'EXTENSIONS DIEDRALES

DE DEGRE $2p$ D'UN CORPS LOCAL

Soutenue le 31 mai 1972 devant la Commission d'examen

C. CHABAUTY	Président	F. BERTRANDIAS	
		J. MARTINET	Examineurs
		J.J. PAYAN	

THÈSE
DE DOCTORAT DE TROISIÈME CYCLE DE MATHÉMATIQUES PURES
présentée
A L'UNIVERSITÉ SCIENTIFIQUE ET MÉDICALE
DE GRENOBLE

par

Marie-Josée FERTON

SUR L'ANNEAU DES ENTIERS D'EXTENSIONS CYCLIQUES
DE DEGRE p ET D'EXTENSIONS DIÉDRALES
DE DEGRE $2p$ D'UN CORPS LOCAL

Soutenue le 31 mai 1972 devant la Commission d'examen
C. CHABAUTY Président F. BERTRANDIAS
J. MARTINET Examineurs
J.J. PAYAN

SOMMAIRE

Pages

INTRODUCTION

CHAPITRE I : RAPPELS ET GENERALITES

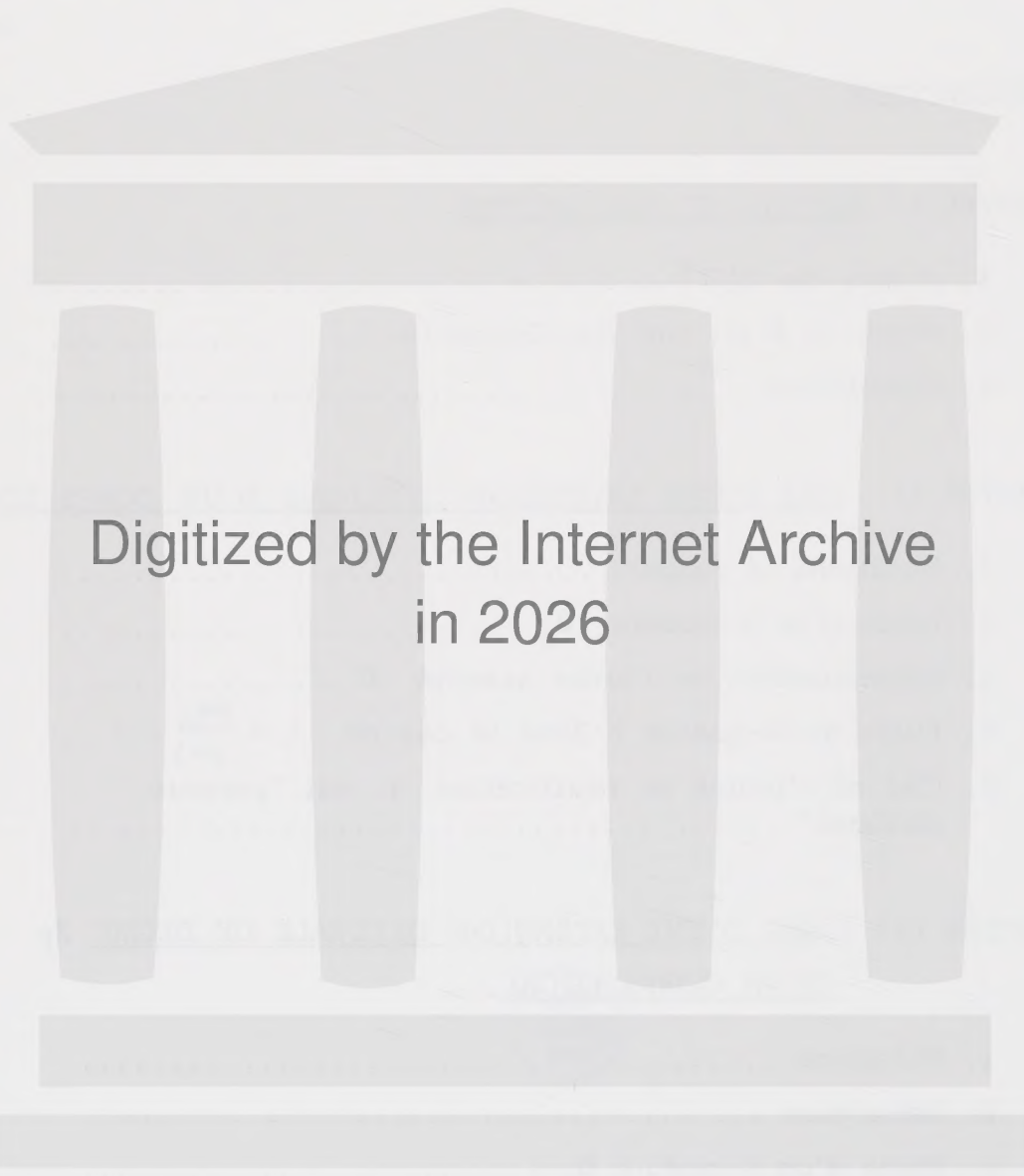
1. Ordres de $k[G]$	1
2. Etude de B en tant que $\mathfrak{D}$ -module	3
3. Complétion	6

CHAPITRE II : CAS D'UNE EXTENSION CYCLIQUE D'UN CORPS LOCAL.

1. Notations et rappels	12
2. Etude d'un A-module $\mathfrak{U}_\theta$	13
3. Détermination de l'ordre associé $\mathfrak{D}$	19
4. Etude du $\mathfrak{D}$ -module B dans le cas où : $t < \frac{pe_0}{p-1} - 1$..	21
5. Cas où l'indice de ramification t est "presque maximal"	25

CHAPITRE III : CAS D'UNE EXTENSION DIEDRALE DE DEGRE $2p$ D'UN CORPS LOCAL.

1. Notations	46
2. Remarques	47
3. Etude d'un A-module $\mathfrak{U}_\theta$	51
4. Etude de l'égalité : $\mathfrak{U}_\theta = \mathfrak{D}$	57
5. Détermination de l'ordre associé $\mathfrak{D}$	63
6. Etude du $\mathfrak{D}$ -module C	67



Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41544304_0005

INTRODUCTION

L'étude des extensions galoisiennes, K/k , de corps de nombres, pour lesquelles l'anneau des entiers de K possède une base normale, remonte à D. Hilbert. On trouve dans le "Zahlbericht" (théorème 132) un résultat que J. Martinet énonce dans [8] sous la forme suivante : "Si K est une extension abélienne modérément ramifiée du corps $\mathbb{Q}$ des rationnels, l'anneau des entiers de K possède, sur $\mathbb{Z}$, une base normale".

Plus généralement, soient A un anneau de Dedekind et k son corps des quotients. K étant une extension galoisienne de k , de groupe de Galois G , appelons B la clôture intégrale de A dans K . Le groupe de Galois G , opère sur B ; on peut donc munir B d'une structure de $A[G]$ -module. Dire que B possède une base normale sur A , c'est dire que B est un $A[G]$ -module libre de rang un.

Pour que B soit libre sur $A[G]$, il est nécessaire que l'extension K/k soit modérément ramifiée; en effet, dans [8], J. Martinet montre que B est un $A[G]$ -module projectif si et seulement si K/k est modérément ramifiée.

Cette condition sur la ramification de K/k n'est pas, en général, une condition suffisante pour que B soit libre sur $A[G]$. Mais, si k est un corps local, E. Noether a montré, ([10]), que B est un $A[G]$ -module libre si et seulement si l'extension K/k est modérément ramifiée.

Pour étudier la structure de B , sans faire d'hypothèses sur la ramification dans K/k , J. Martinet ([9]) a introduit, comme l'avait fait H.W. Leopoldt ([6]) dans le cas d'extensions abéliennes de $\mathbb{Q}$, l'anneau $\mathfrak{O}$ des éléments λ de l'algèbre $k[G]$ tels que : $\lambda B \subset B$.

$\mathfrak{O}$ est un ordre de A dans $k[G]$, on l'appelle l'ordre associé à B dans $k[G]$. On montre ([9]) que $\mathfrak{O}$ est égal à $A[G]$ si et seulement si K/k est modérément ramifiée.

B se trouve donc muni d'une structure de $\mathfrak{O}$ -module. On est alors amené à chercher pour quelles extensions K/k B est un $\mathfrak{O}$ -module libre.

Si G est abélien et si k est le corps $\mathbb{Q}$ des rationnels, H.W. Leopoldt ([6]) montre que B est libre sur $\mathfrak{O}$. Ce résultat généralise le théorème 132 de Hilbert cité plus haut.

A.M. Bergé considère dans [1] le cas où G est un groupe diédral d'ordre $2p$ (p nombre premier impair) et montre en particulier que si $k = \mathbb{Q}$, B est libre sur $\mathfrak{O}$.

Dans [9], J. Martinet pose également la question suivante : B est-il, dans tous les cas, un $\mathfrak{O}$ -module projectif ?

Le but de ce travail est l'étude, en tant que $\mathfrak{O}$ -module, de l'anneau des entiers B de certaines extensions d'un corps local k . Plus précisément, si A désigne un anneau local, on se propose de caractériser les extensions cycliques de degré p et les extensions diédrales de degré $2p$ pour lesquelles B est libre sur $\mathfrak{O}$, (p étant la caractéristique du corps résiduel de k).

.../...

Dans le chapitre I, A désigne un anneau de Dedekind quelconque. Pour pouvoir étudier B comme $\mathfrak{O}$ -module, nous définissons, (cf. [6]), un idéal à gauche de $\mathfrak{O}$, $\mathfrak{A}$, isomorphe à B en tant que $\mathfrak{O}$ -module. B est alors un $\mathfrak{O}$ -module libre si, et seulement si, $\mathfrak{A}$ est un idéal principal de $\mathfrak{O}$. A la fin du chapitre, nous étudions ce que deviennent les propriétés de B comme $\mathfrak{O}$ -module lorsque l'on complète par rapport à certains idéaux premiers de B . On en déduit que, sous des conditions précises, certains résultats obtenus dans le cas local peuvent s'étendre au cas global.

L'étude d'une extension cyclique de degré premier p fait l'objet du chapitre II, A étant dans ce chapitre un anneau local. Nous déterminons pour ces extensions l'ordre $\mathfrak{O}$ associé à B . Nous montrons que la nature de B en tant que $\mathfrak{O}$ -module dépend du nombre de ramification t de l'extension K/k ; en effet, les extensions K/k pour lesquelles B est libre sur $\mathfrak{O}$ peuvent être caractérisées par des conditions arithmétiques portant sur les entiers t et p . Plus précisément, grâce à la collaboration de Monsieur J.P. Bertrandias, nous avons pu exprimer ces conditions au moyen du développement en fraction continue du nombre $\frac{t}{p}$. Nous donnons ainsi des exemples d'extensions où B n'est pas libre sur $\mathfrak{O}$. J. Martinet nous a fait remarquer qu'avec les hypothèses du chapitre II, $\mathfrak{O}$ est un anneau semi-local et que B est un $\mathfrak{O}$ -module libre si et seulement si B est un $\mathfrak{O}$ -module projectif. Nous donnons donc, également, des exemples d'extensions K/k où l'anneau des entiers B de K n'est pas projectif sur $\mathfrak{O}$; ceci permet de répondre à la question posée dans [9].

Dans le chapitre III, nous considérons des extensions diédrales de degré $2p$ d'un corps local. L'étude est analogue à celle faite dans le chapitre précédent pour les extensions cycliques de degré p ; elle fait intervenir les deux nombres de ramification d'une extension diédrale. Il reste dans ce chapitre un cas particulier où le problème n'est pas résolu. Des méthodes identiques à celles employées dans la fin du chapitre II permettront probablement de résoudre ce cas restant.

Les résultats exposés dans ce travail font l'objet de trois notes aux comptes rendus de l'Académie des Sciences :

■ Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local (I). Séance du 17 avril 1972 (F. Bertrandias, M.J. Ferton).

■ Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local (II). Séance du 17 avril 1972 (F. Bertrandias, J.P. Bertrandias, M.J. Ferton).

■ Sur l'anneau des entiers d'une extension diédrale de degré $2p$ d'un corps local. Séance du 15 mai 1972 (M.J. Ferton).

Madame F. BERTRANDIAS a eu l'idée de cette étude et m'en a facilité la réalisation par ses conseils et une participation constante ; ma dette envers elle est immense, qu'elle trouve ici l'expression de toute ma reconnaissance.

Je dois à Monsieur C. CHABAUTY des conditions de travail très favorables ; la présidence de ce jury qu'il a bien voulu accepter m'honore profondément. Toute ma gratitude lui est acquise.

Je remercie très vivement Messieurs J.J. PAYAN et J. MARTINET de s'être intéressés à mon travail et d'avoir accepté de participer à ce jury.

Madame GUTTIN-LOMBARD s'est chargée de l'impression de ce texte avec une patience considérable et beaucoup de compétence, je l'en remercie sincèrement ainsi que Messieurs GAUDE et GIRARD à qui je dois la réalisation matérielle de ce manuscrit.

CHAPITRE I

RAPPELS ET GENERALITES

1. ORDRES DE $k[G]$.

Dans ce chapitre, désignons par A un anneau de Dedekind, par k son corps des fractions, et, par K une extension galoisienne finie de k . On note G le groupe de Galois de K/k , et, B la clôture intégrale de A dans K .

1.1. Rappelons qu'il existe toujours une base normale pour une telle extension K/k , c'est-à-dire qu'il existe un élément θ de B , tel que $\{g.\theta\}_{g \in G}$ soit une base de K/k . En d'autres termes, si $k[G]$ est l'algèbre du groupe G , K est un $k[G]$ -module à gauche libre de rang 1 .

1.2. On appelle ordre de A dans l'algèbre de groupe $k[G]$, un sous-anneau de $k[G]$ contenant une base de $k[G]$ sur k et dont tous les éléments sont entiers sur A [3] .

$A[G]$ est un ordre de A dans $k[G]$; en effet, $A[G]$ est un sous-anneau de $k[G]$ contenant une base de $k[G]$ sur k , et $A[G]$ est entier sur A en tant que A -module de type fini.

Un ordre $\mathfrak{O}_m$ est dit maximal s'il n'est contenu dans aucun ordre de A dans $k[G]$ autre que lui-même [3] .

On sait que tout ordre est contenu dans un ordre maximal.

Dans le cas où G est un groupe abélien, on montre qu'il n'y a qu'un ordre maximal $\mathfrak{O}_m$.

1.3. Ordre associé à B dans $k[G]$.

Considérons le sous-anneau de $k[G]$ défini par :

$$\mathfrak{O} = \{\lambda \in k[G] ; \lambda B \subset B\} \quad [9] .$$

Montrons que $\mathfrak{O}$ est un ordre de A dans $k[G]$; nous l'appellerons l'ordre associé à B dans $k[G]$. $\mathfrak{O}$ est un sous-anneau de $k[G]$, contenant $A[G]$. Si θ est un élément de B engendrant une base normale $(g.\theta)_{g \in G}$ de K/k , et, si d_θ est le discriminant de cette base on a :

$$d_\theta \mathfrak{O} \subset A[G] .$$

En effet, soit λ un élément de $\mathfrak{O}$, $\lambda = \sum_{g \in G} \lambda_g g$ (λ_g dans k pour tout g dans G) . Par définition de $\mathfrak{O}$, $\lambda.\theta$ est dans B ; on en déduit que pour tout g dans G , $d_\theta \lambda_g$ est dans A et que par suite $d_\theta \lambda$ est dans $A[G]$. Cette inclusion entraîne que $\mathfrak{O}$ est entier sur A . En effet, si λ est dans $\mathfrak{O}$, $d_\theta \lambda^n$ est dans $A[G]$ pour tout entier n positif. $A[G]$ étant un A -module noethérien, la suite croissante des sous- A -modules de $A[G]$ engendrés respectivement par : $(d_\theta \lambda)(d_\theta \lambda, d_\theta \lambda^2) \dots (d_\theta \lambda, d_\theta \lambda^2, \dots, d_\theta \lambda^n) \dots$ est stationnaire. Il existe donc un entier positif r , tel que :

$$d_\theta \lambda^r = \sum_{i=1}^{r-1} a_i d_\theta \lambda^i \quad \text{avec } a_i \text{ dans } A \text{ pour } 1 \leq i \leq r-1 ;$$

D'où $\lambda^r = \sum_{i=1}^{r-1} a_i \lambda^i$ avec a_i dans A ; c'est-à-dire que λ est entier sur A

Soit M un $A[G]$ -module de type fini, sans A -torsion, de rang r , c'est-à-dire tel que le $k[G]$ -module : $M_k = k \otimes_A M$ soit libre avec r générateurs. On peut définir de manière analogue l'ordre à gauche associé à M dans $k[G]$; c'est-à-dire l'ensemble des λ de $k[G]$ tels que pour tout x de M λx soit dans M .

1.4. Structure de B comme $\mathfrak{O}$ -module et exemples.

Le groupe de Galois G opérant sur B , B est muni d'une structure de $A[G]$ -module à gauche .

On sait que B est projectif sur $A[G]$ si et seulement si K/k est modérément ramifiée [8] . Si k est un corps local B/A possède une base normale, (c'est-à-dire B est $A[G]$ -libre), si et seulement si, K/k est modérément ramifiée [10] .

D'après la définition de l'ordre associé $\mathfrak{D}$, B est muni également d'une structure de $\mathfrak{D}$ -module à gauche. Si la caractéristique de k est non nulle, $\mathfrak{D}$ coïncide avec $A[G]$ si et seulement si K/k est modérément ramifiée [9]. Si l'on ne veut pas faire d'hypothèses sur la ramification dans K/k , il faut donc étudier B en tant que $\mathfrak{D}$ -module à gauche.

On sait en particulier que B est libre sur $\mathfrak{D}$ dans les deux cas suivants (cf. introduction) :

- $k = \mathbb{Q}$ et G est abélien [6]
- $k = \mathbb{Q}$ et G est un groupe diédral d'ordre $2p$ [1].

Pour étudier B en tant que $\mathfrak{D}$ -module, nous allons introduire dans le paragraphe 2 un sous- $\mathfrak{D}$ -module de $k[G]$, $\mathfrak{U}_\theta$, isomorphe à B (cf. [6]).

2. ETUDE DE B EN TANT QUE $\mathfrak{D}$ -MODULE.

2.1. Définition et propriétés de $\mathfrak{U}_\theta$.

Soit θ un élément de B engendrant une base normale, $(g.\theta)_{g \in G}$, de K/k . On désigne par $\mathfrak{U}_\theta$, le sous $A[G]$ -module de $k[G]$ défini par :

$$\mathfrak{U}_\theta = \{\lambda \in k[G] ; \lambda \theta \in B\}.$$

En utilisant les résultats de [3] on obtient les propriétés suivantes de $\mathfrak{U}_\theta$:

Proposition 1.

- a) $\mathfrak{D}$ est inclus dans $\mathfrak{U}_\theta$, et $\mathfrak{U}_\theta$ est un idéal à gauche de $\mathfrak{D}$.
- b) On a l'égalité : $\mathfrak{U}_\theta.\theta = B$ et l'application φ de $\mathfrak{U}_\theta$ dans B , définie par : $\varphi(\lambda) = \lambda.\theta$ est un isomorphisme de $\mathfrak{D}$ -modules.
- c) $\mathfrak{D}$ est l'ordre à gauche associé à $\mathfrak{U}_\theta$ (cf. §1.3).

Démonstration de la proposition 1 :

a) Les définitions respectives de $\mathfrak{D}$ et de $\mathfrak{U}_\theta$, montrent que $\mathfrak{D}$ est inclus dans $\mathfrak{U}_\theta$ et que $\mathfrak{U}_\theta$ est un $\mathfrak{D}$ -module à gauche. Si l'on note d_θ le discriminant de la base normale de K/k engendré par θ , $(g.\theta)_{g \in G}$, on

voit, pour la même raison que dans le paragraphe 1.3, que :

$$d_{\theta} \mathfrak{A}_{\theta} \subset A[G] .$$

Donc, d_{θ} élément de A est tel que : $d_{\theta} \mathfrak{A}_{\theta} \subset \mathfrak{D}$, et $\mathfrak{A}_{\theta}$ est un idéal à gauche de $\mathfrak{D}$ (cf. [3]).

b) Cette propriété est vraie par définition même de $\mathfrak{A}_{\theta}$.

c) $\mathfrak{A}_{\theta}$ étant contenu dans $k[G]$, on peut définir l'ordre à gauche $\mathfrak{D}'$, associé à $\mathfrak{A}_{\theta}$ (cf. paragraphe 1.3). On a :

$$\mathfrak{D}' = \{ \lambda \in k[G] ; \lambda \mathfrak{A}_{\theta} \subset \mathfrak{A}_{\theta} \} .$$

$\mathfrak{A}_{\theta}$ est un $\mathfrak{D}$ -module à gauche (proposition 1-a)) on en déduit que :

$$\mathfrak{D} \subset \mathfrak{D}' .$$

D'autre part, si un λ de $k[G]$ vérifie : $\lambda \mathfrak{A}_{\theta} \subset \mathfrak{A}_{\theta}$, comme on a :

$B = \mathfrak{A}_{\theta} \theta$, λ vérifie aussi $\lambda B \subset B$. Par suite $\mathfrak{D}' \subset \mathfrak{D}$. $\mathfrak{D}$ est donc l'ordre à gauche associé à $\mathfrak{A}_{\theta}$.

Remarque :

Si B est un $\mathfrak{D}$ -module libre, ce module est de rang 1. En effet, K est un $k[G]$ -module libre de rang 1.

2.2. Proposition 2.

Les quatres assertions suivantes sont équivalentes :

- (i) B est un $\mathfrak{D}$ -module libre,
- (ii) il existe θ tel que : $\mathfrak{D} = \mathfrak{A}_{\theta}$,
- (iii) il existe θ tel que $\mathfrak{A}_{\theta}$ soit un anneau,
- (iv) pour tout θ , $\mathfrak{A}_{\theta}$ est un idéal à gauche, principal de $\mathfrak{D}$.

Démonstration de la proposition 2 :

(i) équivalent à (ii). Si B est $\mathfrak{D}$ -libre, il existe α dans B tel que $B = \mathfrak{D} \cdot \alpha$ et par suite $\mathfrak{D} = \mathfrak{A}_{\alpha}$.

Réciproquement, s'il existe θ tel que $\mathfrak{D} = \mathfrak{A}_{\theta}$ on a : $B = \mathfrak{D} \cdot \theta$.

(ii) équivaut à (iii) . Si $\mathcal{O} = \mathfrak{u}_\theta$, $\mathfrak{u}_\theta$ est un anneau.

Réciproquement, si θ est tel que $\mathfrak{u}_\theta$ soit un anneau, montrons que $\mathfrak{u}_\theta$ est un ordre de $k[G]$. $\mathfrak{u}_\theta$ contient $A[G]$ et $d_\theta \mathfrak{u}_\theta \subset A[G]$, on en déduit, comme pour l'ordre associé dans le paragraphe 1.3 que $\mathfrak{u}_\theta$ est entier sur A . B est donc libre sur l'ordre $\mathfrak{u}_\theta$; or, si B est libre sur un ordre de A dans $k[G]$, cet ordre est nécessairement l'ordre associé à B dans $k[G]$ [9]. On en déduit que $\mathcal{O} = \mathfrak{u}_\theta$.

(i) équivaut à (iv) . Si B est libre sur $\mathcal{O}$, il existe α dans B tel que : $B = \mathcal{O}.\alpha$. Quel que soit θ engendrant une base normale de K/k on a alors :

$$\mathcal{O}.\alpha = \mathfrak{u}_\theta.\theta .$$

Il existe donc φ dans $\mathfrak{u}_\theta$ tel que $\alpha = \varphi.\theta$ et par suite $\mathfrak{u}_\theta = \mathcal{O}\varphi$.

Réciproquement, si $\mathfrak{u}_\theta = \mathcal{O}\varphi$ pour un φ de $\mathfrak{u}_\theta$ on a : $B = \mathcal{O}\varphi.\theta$.

2.3. Proposition 3.

Si k est un corps local et G un groupe abélien, B est un $\mathcal{O}$ -module libre si, et seulement si, B est un $\mathcal{O}$ -module projectif.

Démonstration de la proposition 3 :

Si A est un anneau local et G un groupe abélien, l'ordre $\mathcal{O}$ associé à B est un anneau semi-local en tant que A -module de type fini. ([2] chap.IV §2 n°5 cor.3 de la prop.9).

Dans ce cas, si B est un $\mathcal{O}$ -module projectif, B est un $\mathcal{O}$ -module de rang défini et égal à 1 (définition de [2] chap.II §5 n°3) ; en effet, quel que soit $\mathfrak{p}$, idéal premier de $\mathcal{O}$, $B_{\mathfrak{p}}$ est isomorphe à un idéal de $\mathcal{O}_{\mathfrak{p}}$ (où $B_{\mathfrak{p}}$ et $\mathcal{O}_{\mathfrak{p}}$ sont les localisés en $\mathfrak{p}$ de B et de $\mathcal{O}$). Par suite $B_{\mathfrak{p}}$ est un $\mathcal{O}_{\mathfrak{p}}$ -module libre de rang 1 .

Un module projectif sur un anneau semi-local, de rang défini, est libre d'après [2] (chap.II §5 n°4 prop.5).

Par conséquent, dans les conditions de la proposition 3, si B est un $\mathcal{O}$ -module projectif, B est aussi un $\mathcal{O}$ -module libre.

3. COMPLETION.

3.1. Dans ce paragraphe, on suppose que K et k sont des corps de nombres, et que $\mathfrak{p}$ est un idéal premier de K dont le groupe de décomposition coïncide avec G . On note $\mathfrak{p} = \mathfrak{p} \cap A$, $\mathfrak{p}$ est donc le seul idéal premier au-dessus de $\mathfrak{p}$.

$|\cdot|_{\mathfrak{p}}$ désigne une valeur absolue de K , associée à l'idéal $\mathfrak{p}$.

$K_{\mathfrak{p}}$ et $k_{\mathfrak{p}}$ désignent respectivement les corps complétés de K et de k pour cette valeur absolue.

$B_{\mathfrak{p}}$ et $A_{\mathfrak{p}}$ sont les anneaux d'entiers respectifs de $K_{\mathfrak{p}}$ et de $k_{\mathfrak{p}}$. Si θ engendre une base normale de K/k , θ engendre également une base normale de $K_{\mathfrak{p}}/k_{\mathfrak{p}}$.

On note :

$$\mathfrak{D} = \{\lambda \in k_{\mathfrak{p}}[G] ; \lambda B_{\mathfrak{p}} \subset B_{\mathfrak{p}}\}.$$

$$\mathfrak{U}_{\theta} = \{\lambda \in k_{\mathfrak{p}}[G] ; \lambda \theta \in B_{\mathfrak{p}}\}.$$

Pour tout élément λ de l'algèbre $k_{\mathfrak{p}}[G]$, posons :

$$\|\lambda\|_{\mathfrak{p}} = \sup_{\beta \in B_{\mathfrak{p}}^*} \frac{|\lambda \beta|_{\mathfrak{p}}}{|\beta|_{\mathfrak{p}}}.$$

On vérifie que $\|\cdot\|_{\mathfrak{p}}$ est une norme de $k_{\mathfrak{p}}[G]$ -algèbre et que $k_{\mathfrak{p}}[G]$ est le complété de $k[G]$ pour cette norme. On obtient alors les résultats suivants :

3.2. Proposition 4.

$\mathfrak{D}$ et $\mathfrak{U}_{\theta}$ sont les complétés respectifs de $\mathfrak{D}$ et de $\mathfrak{U}_{\theta}$, dans $k_{\mathfrak{p}}[G]$ pour la norme $\|\cdot\|_{\mathfrak{p}}$.

Démonstration de la proposition 4 :

Nous allons montrer successivement que $\mathfrak{D}$ est inclus dans $\mathfrak{D}$, que $\mathfrak{D}$ est fermé dans $k_{\mathfrak{p}}[G]$ pour la norme $\|\cdot\|_{\mathfrak{p}}$, et, que $\mathfrak{D}$ est dense dans $\mathfrak{D}$ pour cette même norme.

$\mathfrak{D}$ est inclus dans $\tilde{\mathfrak{D}}$: $k[G]$ est inclus dans $k_p[G]$. Si un élément λ de $k[G]$ vérifie $\lambda.B \subset B$ montrons que $\lambda.B_p \subset B_p$. Tout élément β de B_p est limite d'une suite de Cauchy $\{\beta_n\}$ de B . Pour tout entier n : $\lambda.\beta_n \in B$, et, la suite $\{\lambda.\beta_n\}$ est de Cauchy car :

$$|\lambda.\beta_n|_p \leq \|\lambda\|_p |\beta_n|_p.$$

La limite de cette suite, $\lambda.\beta$ est donc dans B_p .

$\tilde{\mathfrak{D}}$ est fermé dans $k_p[G]$: soit μ un élément de $k_p[G]$ adhérent à $\tilde{\mathfrak{D}}$. Il existe dans $\tilde{\mathfrak{D}}$ un élément λ tel que : $\|\lambda - \mu\|_p \leq 1$, alors μ est dans $\tilde{\mathfrak{D}}$. En effet : $\mu.B_p = \lambda.B_p - (\lambda - \mu).B_p$. λ étant dans $\tilde{\mathfrak{D}}$:

$$\lambda.B_p \subset B_p.$$

D'autre part, $|(\lambda - \mu).\beta|_p \leq |\beta|_p \leq 1$ pour tout β dans B_p , on a donc :

$$(\lambda - \mu).B_p \subset B_p.$$

Par suite :

$$\mu.B_p \subset B_p.$$

$\mathfrak{D}$ est dense dans $\tilde{\mathfrak{D}}$. Soit λ un élément de $\tilde{\mathfrak{D}}$. $k[G]$ étant dense dans $k_p[G]$, il existe pour tout ε positif un élément λ' de $k[G]$ vérifiant :

$$\|\lambda - \lambda'\|_p \leq \varepsilon.$$

En particulier, on peut choisir λ' tel que $\|\lambda - \lambda'\|_p \leq 1$; comme précédemment on en déduit que : $(\lambda - \lambda').B_p \subset B_p$ et que λ' est dans $\tilde{\mathfrak{D}}$. λ' est dans $k[G]$ et dans $\tilde{\mathfrak{D}}$, c'est donc un élément de $\mathfrak{D}$.

De manière analogue on montre que $\mathfrak{U}_\theta$ est inclus dans $\tilde{\mathfrak{U}}_\theta$, que $\tilde{\mathfrak{U}}_\theta$ est fermé dans $k_p[G]$ pour la norme $\|\cdot\|_p$, et, que $\mathfrak{U}_\theta$ est dense dans $\tilde{\mathfrak{U}}_\theta$ pour cette même norme.

3.3. Proposition 5.

Si B est un $\mathfrak{D}$ -module libre (respectivement projectif), B_p est un $\tilde{\mathfrak{D}}$ -module libre (respectivement projectif).

Démonstration de la proposition 5 :

a) si B est $\mathfrak{D}$ -module libre, il existe dans $\mathfrak{U}_\theta$ un élément φ , tel que : $\mathfrak{U}_\theta = \mathfrak{D}\varphi$. On en déduit que $\mathfrak{D} = \mathfrak{U}_{\varphi, \theta}$. La proposition 4 nous permet alors d'écrire :

$$\tilde{\mathfrak{D}} = \tilde{\mathfrak{U}}_{\varphi, \theta}, \text{ c'est-à-dire } \tilde{\mathfrak{U}}_\theta = \tilde{\mathfrak{D}}\varphi.$$

$B_{\mathfrak{P}}$ est donc un $\tilde{\mathfrak{D}}$ -module libre.

b) $\mathfrak{U}_\theta$ est un $\mathfrak{D}$ -module de type fini, il existe donc des éléments : $\mu_1, \mu_2, \dots, \mu_n$ de $\mathfrak{U}_\theta$ tels que : $\mathfrak{U}_\theta = \mathfrak{D}\mu_1 + \mathfrak{D}\mu_2 + \dots + \mathfrak{D}\mu_n$.

Soit $L = \mathfrak{D}^n$ et soit ψ l'application de L dans $\mathfrak{U}_\theta$ définie par :

$$\psi(x) = \sum_{i=1}^n x_i \mu_i, \quad x = (x_1, x_2, \dots, x_n) \text{ étant dans } L.$$

Si N est le noyau de ψ dans L , on peut écrire la suite exacte suivante :

$$0 \rightarrow N \rightarrow L \xrightarrow{\psi} \mathfrak{U}_\theta \rightarrow 0.$$

Si B est un $\mathfrak{D}$ -module projectif, $\mathfrak{U}_\theta$ est un $\mathfrak{D}$ -module projectif, et, la suite exacte précédente se scinde. Il existe donc dans L un sous- $\mathfrak{D}$ -module M , isomorphe à $\mathfrak{U}_\theta$ et tel que :

$$L = M \oplus N.$$

Posons $\mathfrak{a} = k[G]$, $L_k = \mathfrak{a}^n$ et prolongeons l'application ψ de L dans $\mathfrak{U}_\theta$ par une application ψ' de L_k dans $\mathfrak{a}$ définie par :

$$\psi'(x) = \sum_{i=1}^n x_i \mu_i, \quad x = (x_1, x_2, \dots, x_n) \text{ étant un élément de } L_k.$$

Soit $N_k = \{x = (x_i)_{1 \leq i \leq n} \in L_k ; \sum_{i=1}^n x_i \mu_i = 0\}$ le noyau de ψ' . On a :

$$0 \rightarrow N_k \rightarrow L_k \xrightarrow{\psi'} \mathfrak{a} \rightarrow 0.$$

Si x est un élément de L_k , il existe d dans A tel que dx soit dans L , c'est-à-dire : $L_k = k \otimes_A L$. De même, si x est dans N_k , il existe d dans A tel que dx soit dans N , c'est-à-dire : $N_k = k \otimes_A N$. Soit alors $M_k = \{\frac{1}{d}M, d \in k^*\} = k \otimes_A M$ le sous- $\mathfrak{a}$ -module de L_k engendré par M ; on a $L_k = M_k \oplus N_k$ et M_k isomorphe à $\mathfrak{a}$. (cf [2 bis] §1 et 2).

Pour tout élément $x = (x_i)_{1 \leq i \leq n}$ de L_k posons :

$$\|x\|^* = \max_{1 \leq i \leq n} \|x_i\|_{\mathfrak{P}} ;$$

$\|\cdot\|^*$ est une norme sur L_k .

Montrons que la norme $\|\cdot\|_{\mathfrak{P}}$ sur $\mathfrak{a} = k[G]$, et, que la norme sur M_k induite par la norme $\|\cdot\|^*$ de L_k , sont équivalentes.

M_k étant isomorphe à $\mathfrak{a}$, il existe un élément $u = (u_1, u_2, \dots, u_n)$ de M_k tel que :

$$M_k = \{\rho u, \rho \in \mathfrak{a}\} .$$

D'autre part, comme ψ' est surjective, il existe ρ_0 dans $\mathfrak{a}$ tel que $\psi'(\rho_0 u) = \sum_{i=1}^n \rho_0 u_i \mu_i = \rho_0 \sum_{i=1}^n u_i \mu_i = 1$. Posons $v = \rho_0 u = (\rho_0 u_1, \dots, \rho_0 u_n)$, M_k peut s'écrire : $M_k = \{\rho' v ; \rho' \in \mathfrak{a}\}$.

En effet, si $x = (x_1, x_2, \dots, x_n)$ est dans M_k , il existe ρ dans $\mathfrak{a}$ tel que pour $1 \leq i \leq n$:

$$x_i = \rho u_i = (\rho \rho_0^{-1}) \rho_0 u_i = \rho' v_i \text{ avec } \rho' = \rho \rho_0^{-1}$$

et

$$x = \rho' v .$$

Pour tout élément x de M_k , $x = \rho v$ (ρ dans $\mathfrak{a}$) on a :

$$\|x\|^* = \max_{1 \leq i \leq n} \|\rho v_i\|_{\mathfrak{P}}$$

et si l'on pose $c = \max_{1 \leq i \leq n} \|v_i\|_{\mathfrak{P}}$ on a : $\|x\|^* \leq c \|\rho\|_{\mathfrak{P}}$.

Inversement pour tout élément ρ de $\mathfrak{a}$ on a :

$$\rho = \rho \sum_{i=1}^n v_i \mu_i = \sum_{i=1}^n x_i \mu_i \text{ si } x = \rho v .$$

Et par suite, en posant $c' = \sum_{i=1}^n \|\mu_i\|_{\mathfrak{P}}$ on obtient :

$$\|\rho\|_{\mathfrak{P}} \leq c' \|x\|^* .$$

Les normes $\| \cdot \|_k^*$ sur M_k et $\| \cdot \|_{\mathfrak{P}}$ sur $\mathfrak{a}$ étant équivalentes, les normes induites sur M et $\mathfrak{U}_\theta$ le sont. Soit $\tilde{M}_k$ le complété de M_k pour la norme $\| \cdot \|_k^*$, et $\tilde{M}$ le complété de M pour cette même norme. $\tilde{M}_k$ et $\tilde{\mathfrak{a}} = k_p[G]$ sont isomorphes en tant que $\tilde{\mathfrak{a}}$ -modules et $\tilde{M}$ et $\tilde{\mathfrak{U}}_\theta$ sont isomorphes en tant que $\tilde{\mathfrak{S}}$ -modules.

Montrons que : $\tilde{L}_k = \tilde{M}_k \oplus \tilde{N}_k$, $\tilde{L}_k$ et $\tilde{N}_k$ étant les complétés de L_k et N_k pour la norme $\| \cdot \|_k^*$. Si l'on note, $\text{Card } G$, l'ordre de G , L_k est un k -espace vectoriel de dimension $n \times \text{Card } G$, $\tilde{L}_k = \tilde{\mathfrak{a}}^n$ est un k_p -espace vectoriel de dimension $n \times \text{Card } G$, d'après les hypothèses faites en début de paragraphe sur l'idéal $\mathfrak{P}$.

$\tilde{M}_k$ étant isomorphe à $\tilde{\mathfrak{a}}$, c'est un sous-espace vectoriel de dimension $\text{Card } G$ sur k_p . D'autre part, la dimension de $\tilde{N}_k$ sur k_p en tant qu'espace vectoriel, est inférieure ou égale à celle de N_k sur k , c'est-à-dire $(n-1) \times \text{Card } G$. Pour montrer que : $\tilde{L}_k = \tilde{M}_k \oplus \tilde{N}_k$ il nous suffit donc de montrer que : $\tilde{L}_k = \tilde{M}_k + \tilde{N}_k$. Comme on a : $L_k = M_k \oplus N_k$, il nous reste à montrer que la projection sur M_k , d'une suite de Cauchy de L_k est une suite de Cauchy de M_k .

Soit $\{x^{(m)}\}_{m \in \mathbb{N}}$ une suite de Cauchy dans L_k avec $x^{(m)} = y^{(m)} + z^{(m)}$ où $\{y^{(m)}\}$ est une suite de M_k et $\{z^{(m)}\}$ une suite de N_k .

Si $x^{(m)} = (x_i^{(m)})_{1 \leq i \leq n}$, $y^{(m)} = (y_i^{(m)})_{1 \leq i \leq n}$ et $y^{(m)} = \rho_m v$, $\{\rho_m\}$ étant une suite de $\mathfrak{a}$, on a :

$$\rho_m = \sum_{i=1}^n y_i^{(m)} \mu_i = \sum_{i=1}^n x_i^{(m)} \mu_i \quad \text{et donc : } \|\rho_m\|_{\mathfrak{P}} \leq c' \|x^{(m)}\|_k^*.$$

ρ_m est donc une suite de Cauchy dans $\mathfrak{a}$ et $y^{(m)}$ une suite de Cauchy dans M_k . $z^{(m)} = x^{(m)} - y^{(m)}$ est donc une suite de Cauchy dans N_k .

$\tilde{L}_k = \tilde{M}_k \oplus \tilde{N}_k$ entraîne : $\tilde{L} = \tilde{M} \oplus \tilde{N}$, où $\tilde{L}$, $\tilde{M}$ et $\tilde{N}$ sont les complétés respectifs de L , M et N pour les normes $\| \cdot \|_k^*$.

En effet : $\tilde{M} \cap \tilde{N} \subset \tilde{M}_k \cap \tilde{N}_k = \{0\}$. D'autre part, comme $L = M \oplus N$ et que $\tilde{L}_k = \tilde{M} \oplus \tilde{N}_k$ on peut montrer que la projection sur M d'une suite de Cauchy de L est une suite de Cauchy, on en déduit que $\tilde{L} = \tilde{M} + \tilde{N}$.

$\tilde{\mathfrak{U}}_\theta$ étant isomorphe à $\tilde{M}$ en tant que $\tilde{\mathfrak{D}}$ -module, et $\tilde{M}$ étant facteur direct du $\tilde{\mathfrak{D}}$ -module libre $\tilde{L}$, $\tilde{\mathfrak{U}}_\theta$ est un $\tilde{\mathfrak{D}}$ -module projectif. On a donc montré que si B est un $\mathfrak{D}$ -module projectif, $B_{\mathfrak{P}}$ est un $\tilde{\mathfrak{D}}$ -module projectif.

Ceci achève la démonstration de la proposition 5.

CHAPITRE II

CAS D'UNE EXTENSION CYCLIQUE

DE DEGRE PREMIER DE CORPS LOCAUX

1. NOTATIONS ET RAPPELS.

1.1. Dans le chapitre II, k désigne un corps local de caractéristique zéro, et de caractéristique résiduelle le nombre premier p . K est une extension cyclique de degré p de k , et G est le groupe de Galois de K/k . A et B sont les anneaux d'entiers respectifs de k et de K .

On note :

- σ un générateur de G ; f l'élément de $k[G]$ défini par $f = \sigma - 1$;
- ϖ et π , des uniformisantes respectives de k et K ;
- v_k et v_K , les valuations normalisées respectives de k et K ;
- e_o , l'indice de ramification absolu de k : $e_o = v_k(p)$;
- t le nombre de ramification de l'extension K/k c'est-à-dire :

$$t = \left\{ \min_{x \in B^*} v_k(\sigma x - x) \right\} - 1 .$$

On note aussi : pour tout nombre réel x , $[x]$, la partie entière de x et $\underline{x}$, sa partie fractionnaire, de sorte que $x = [x] + \underline{x}$; a le plus petit entier positif ou nul congru à t modulo p ; $a_o = \left[\frac{t}{p} \right]$. Le nombre de ramification s'écrit donc :

$$t = a_o p + a \quad \text{avec} \quad 0 \leq a \leq p-1 .$$

1.2. Pour étudier l'ordre, $\mathfrak{D}$, associé à B et la structure du $\mathfrak{D}$ -module B nous allons déterminer un élément θ de B , engendrant une base normale de K/k et le sous $A[G]$ -module de $k[G]$, $\mathfrak{U}_\theta$, correspondant, (chapitre I, paragraphe 2). L'ordre associé $\mathfrak{D}$ est alors l'ordre à gauche associé à $\mathfrak{U}_\theta$ (prop-

sition 1, chapitre I) et B est libre sur $\mathfrak{O}$ si et seulement si $\mathfrak{A}_\theta$ est un idéal principal de $\mathfrak{O}$ (prop.2, chap.I).

Remarque.

Dans le cas où l'extension K/k est non ramifiée, on a $t = -1$, et on sait que B est un $A[G]$ -module libre, [8], [10] ; par suite $A[G]$ est l'ordre associé à B dans $k[G]$.

Dans cette situation, on peut prendre pour θ une unité de B dont l'image dans le corps résiduel engendre une base normale de l'extension résiduelle, on vérifie alors que : $\mathfrak{O} = \mathfrak{A}_\theta = A[G]$.

On supposera donc dans toute la suite de ce chapitre que K/k est une extension sauvagement ramifiée ($t \geq 1$).

1.3. Rappelons les propriétés suivantes sur le nombre de ramification d'une extension cyclique de corps locaux :

a) t vérifie l'inégalité : $t \leq \frac{pe_o}{p-1}$ d'après [12] chap.IV §2 exercice 3.

b) Réciproquement, étant donné un corps k et un entier t premier à p tel que $-1 \leq t \leq \frac{pe_o}{p-1}$, il existe des extensions K de k , cycliques de degré p , ayant l'entier t comme nombre de ramification. [12] chap.IV §2 exercice 5.

c) Si le nombre de ramification t est divisible par p , k contient les racines p -èmes de l'unité et il existe une uniformisante ϖ de k , telle que : $K = k(\varpi^{1/p})$.

On montre alors que $t = \frac{pe_o}{p-1}$ ([7] théorème 3).

2. ETUDE D'UN A-MODULE $\mathfrak{A}_\theta$.

2.1. Lemme 1.

Si $t \geq 1$ et si x est un élément de B alors :

$$v_K(f.x) = v_K(x) + t, \text{ si } p \text{ ne divise pas } v_K(x).$$

$$v_K(f.x) \geq v_K(x) + t + 1, \text{ si } p \text{ divise } v_K(x).$$

Démonstration :

Posons $\sigma.\pi = \pi(1+u\pi^t)$ et $x = v\pi^r$ où u et v sont des unités de K et où $r = v_K(x)$ est un entier positif.

$$\begin{aligned} f.x &= \sigma.x - x = (\sigma.v)(\sigma.\pi^r) - v\pi^r \\ &= \pi^r [(\sigma v - v) + (\sigma.v)(ru\pi^t + \binom{r}{2}u^2\pi^{2t} + \dots + u^r\pi^{rt})] \end{aligned}$$

Comme $v_K(\sigma v - v) \geq t+1$, on en déduit le lemme 1.

Proposition 1.

a) Si $t \geq 1$ et $t \not\equiv 0$ (modulo p), $\theta = \pi^a$ engendre une base normale de K/k et $\mathfrak{U}_\theta$ est le sous-A-module de $k[G]$ engendré par la famille $(\frac{f^i}{v_i})_{\substack{\mathfrak{w} \\ 0 \leq i \leq p-1}}$, avec $v_i = [\frac{it+a}{p}] = ia_0 + [(i+1)\frac{a}{p}]$.

b) Si $t \equiv 0$ (modulo p) et si $\mathfrak{w}$ et π sont respectivement des uniformisantes de k et de K telles que : $\pi^p = \mathfrak{w}$, $\theta = 1 + \pi + \dots + \pi^{p-1}$ engendre une base normale de K/k et $\mathfrak{U}_\theta$ coïncide avec l'ordre maximal de $k[G]$.

Démonstration de la proposition 1 :

a) Utilisons le lemme 1. Comme a est non nul et premier à p , on a pour tout entier i , $0 \leq i \leq p-1$: $v_K(f^i.\pi^a) = it+a$. C'est-à-dire : $v_K(f^i.\pi^a) \equiv (i+1)a$ (modulo p). Posons : $\theta = \pi^a$. Les p éléments de B , $f^i.\theta$, $0 \leq i \leq p-1$, sont de valuations toutes différentes modulo p . On en déduit que la famille $(\frac{f^i.\theta}{v_i})_{\substack{\mathfrak{w} \\ 0 \leq i \leq p-1}}$, avec $v_i = [\frac{it+a}{p}]$, est une A-base de B ; d'où le a) de la proposition 1.

b) Si $a = 0$, d'après le 1.3, c) du chap.II, k contient les racines p -èmes de l'unité. Il existe $\mathfrak{w}$ et π telles que $\pi^p = \mathfrak{w}$ et t prend la valeur maximum : $\frac{pe}{p-1}$. On a pour $0 \leq i \leq p-1$, $\sigma^i.\pi = \zeta^i\pi$, ζ étant une racine primitive p -ème de l'unité. Considérons alors, dans $k[G]$ la famille définie par : $1_\chi = \frac{1}{p} \sum_{g \in G} \chi(g^{-1}).g$ où χ parcourt le groupe des caractères de G si l'on note χ_i , le caractère de G défini par : $\chi_i(\sigma) = \zeta^i$ pour $0 \leq i \leq p-1$

alors quel que soit i compris entre 0 et $p-1$, on a :

$$1_{\chi_i} = \frac{1}{p} \sum_{j=0}^{p-1} \zeta^{-ji} \sigma^j.$$

On vérifie que les 1_{χ_i} , $0 \leq i \leq p-1$ sont p idempotents de $k[G]$, deux à deux orthogonaux, et que :

$$1 = \sum_{i=0}^{p-1} 1_{\chi_i}.$$

D'autre part, il est facile de voir que pour tout i , $0 \leq i \leq p-1$:

$$1_{\chi_i} \cdot \pi^j = 0 \quad \text{si } j \neq i$$

et

$$1_{\chi_i} \cdot \pi^i = \pi^i.$$

Posons $\theta = 1 + \pi + \dots + \pi^{p-1}$, la famille $(1_{\chi_i} \cdot \theta)_{0 \leq i \leq p-1}$ est une A -base de B . $\mathfrak{U}_\theta$ est donc le sous A -module de $k[G]$ engendré par la famille $(1_{\chi_i})_{0 \leq i \leq p-1}$.

Montrons que ce sous-module est l'ordre maximal de A dans $k[G]$. Comme k contient les racines p -èmes de 1, l'algèbre $k[G]$ est isomorphe à l'algèbre k^p , produit direct de p corps isomorphes à k . De façon plus précise soit φ l'isomorphisme de k -espaces vectoriels de $k[G]$ dans k^p défini par : $\varphi(1_{\chi_i}) = (0, 0, 0, \dots, 1, 0, \dots, 0)$ où 1 est la i -ème place. En écrivant, pour un α de $k[G]$: $\alpha = \sum_{i=0}^{p-1} \alpha_i 1_{\chi_i}$ et en remarquant que : $\sigma^j 1_{\chi_i} = \zeta^{ij} 1_{\chi_i}$, on voit que φ est aussi un isomorphisme de k -algèbres.

L'ordre maximal de l'algèbre k^p étant l'anneau A^p , on a : $\mathfrak{O}_m = \varphi^{-1}(A^p)$. $\mathfrak{O}_m$ est donc bien le sous A -module de $k[G]$ engendré par la famille des 1_{χ_i} , $0 \leq i \leq p-1$.

2.2. Etude de l'égalité : $\mathfrak{U}_\theta = \mathfrak{O}$.

On a évidemment l'inclusion $\mathfrak{O} \subset \mathfrak{U}_\theta$ (proposition 1 Chap.I). D'après la proposition 2 du chapitre I, si $\mathfrak{O} = \mathfrak{U}_\theta$, B est libre sur $\mathfrak{O}$. Déterminons donc dans quels cas l'égalité : $\mathfrak{O} = \mathfrak{U}_\theta$ est vérifiée.

Lemme 2.

Soit M , le sous A -module de $k[G]$ engendré par la famille $(\frac{f^i}{\varpi^{\nu_i}})_{0 \leq i \leq p-1}$, où les entiers ν_i vérifient : $\nu_0 = 0 \leq \nu_1 \leq \nu_2 \leq \dots \leq \nu_{p-1} \leq e_0$.
 M est un sous-anneau de $k[G]$, si et seulement si, pour tout couple (ij) d'entiers compris entre 1 et $p-1$ on a :

- (1) si $i+j \leq p-1$, $\nu_i + \nu_j \leq \nu_{i+j}$
- (2) si $i+j \geq p$, $\nu_i + \nu_j \leq e_0 + \nu_{i+j+1-p}$.

Démonstration :

Les conditions (1) s'obtiennent de manière évidente.

Pour obtenir les conditions (2) remarquons que :

$$(1+f)^p = 1,$$

d'où

$$f^p = -pf^{p-1} - \binom{p}{2}f^{p-2} - \dots - \binom{p}{k}f^{p-k} - \dots - pf.$$

Donc si ν est entier positif, $\frac{f^p}{\varpi^\nu}$ est dans M si et seulement si :

$\nu \leq e_0 + \nu_1$ ($\frac{f^p}{\varpi^{e_0}}$ est une unité de A). On en déduit pour $1 \leq m \leq p-1$:

$$f^{p-1+m} = pr_{p-1}f^{p-1} + pr_{p-2}f^{p-2} + \dots + pr_m f^m + p^2 r_{m-1} f^{m-1} + \dots + p^2 r_1 f$$

les r_i étant des unités de A .

Si ν est un entier positif, $\frac{f^{p-1+m}}{\varpi^\nu}$ est dans M si et seulement si :
 $\nu \leq e_0 + \nu_m$.

On a donc obtenu les conditions (2).

Proposition 2.

Soit θ l'élément défini dans la proposition 1 précédente ; on a l'égalité :
 $\mathfrak{U}_\theta = \mathfrak{D}$, si et seulement si, ou bien $a = 0$ ou bien a divise $p-1$.

Démonstration de la proposition 2 :

On utilise le fait que $\mathfrak{U}_\theta = \mathfrak{D}$ si et seulement si $\mathfrak{U}_\theta$ est un sous-anneau de $k[G]$ (chapitre I, proposition 2).

- Si $a = 0$ on a vu que : $\mathfrak{A}_\theta = \mathfrak{D}_m$ et donc : $\mathfrak{A}_\theta = \mathfrak{D}$.

- Si $a \neq 0$ nous appliquons le lemme 2 précédent, avec $M = \mathfrak{A}_\theta$.

Si $v_i = \left[\frac{it+a}{p} \right]$ et $t = a_0 p + a$, les conditions s'écrivent :

$$(1) \quad \text{si } i+j \leq p-1, \quad \left[(i+1) \frac{a}{p} \right] + \left[(j+1) \frac{a}{p} \right] \leq \left[(i+j+1) \frac{a}{p} \right]$$

$$(2) \quad \text{si } i+j \geq p, \quad \left[(i+1) \frac{a}{p} \right] + \left[(j+1) \frac{a}{p} \right] \leq e_0 - (p-1)a_0 + \left[(i+j+2-p) \frac{a}{p} \right] .$$

La démonstration de la proposition 2 se réduit alors au lemme 3 suivant et au fait que : $a \leq e_0 - (p-1)a_0$ d'après l'inégalité a) du paragraphe 1.3 de ce chapitre.

Lemme 3.

Soit a un entier tel que : $1 \leq a \leq p-1$, et soit (i, j) un couple d'entiers compris entre 1 et $p-1$,

a) si $i+j \geq p$ on a :

$$\left[(i+1) \frac{a}{p} \right] + \left[(j+1) \frac{a}{p} \right] \leq a + \left[(i+j+2-p) \frac{a}{p} \right] ;$$

b) les inégalités $\left[(i+1) \frac{a}{p} \right] + \left[(j+1) \frac{a}{p} \right] \leq \left[(i+j+1) \frac{a}{p} \right]$ sont vérifiées pour tout couple (i, j) tel que : $i+j \leq p-1$, si et seulement si, a divise $p-1$.

Démonstration :

a) si $i+j \geq p$ on a :

$$\left[(i+1) \frac{a}{p} \right] + \left[(j+1) \frac{a}{p} \right] \leq \left[(i+j+2) \frac{a}{p} \right] = a + \left[(i+j+2-p) \frac{a}{p} \right] ;$$

b) - Si $i+j \leq p-1$ et si a divise $p-1$, en posant $a = \frac{p-1}{d}$, d entier positif, on peut écrire :

$$\left[(i+1) \frac{p-1}{dp} \right] + \left[(j+1) \frac{p-1}{dp} \right] = \left[\frac{i}{d} + \frac{p-i-1}{dp} \right] + \left[\frac{j}{d} + \frac{p-j-1}{dp} \right] = \left[\frac{i}{d} \right] + \left[\frac{j}{d} \right]$$

et

$$\left[\frac{i}{d} \right] + \left[\frac{j}{d} \right] \leq \left[\frac{i+j}{d} \right] = \left[(i+j+1) \frac{p-1}{dp} \right] .$$

- Si a ne divise pas $p-1$, montrons qu'il existe un couple (i, j) d'entiers compris entre 1 et $p-1$ tel que $i+j \leq p-1$ et vérifiant :

$$\left[(i+j) \frac{a}{p} \right] + \left[(j+1) \frac{a}{p} \right] > \left[(i+j+1) \frac{a}{p} \right] ;$$

cette dernière égalité est équivalente à :

$$\underbrace{(i+1) \frac{a}{p}} + \underbrace{(j+1) \frac{a}{p}} < \frac{a}{p} + \underbrace{(i+j+1) \frac{a}{p}} . \quad (1)$$

Notons : $\frac{t}{p} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}} = [a_0, a_1, \dots, a_n]$, avec $a_n > 1$, le

développement en fraction continue de $\frac{t}{p}$ et $q_0 = 1$, $q_1 = a_1$, $q_n = p$ les dénominateurs des "réduites" successives.

L'hypothèse a ne divise pas $p-1$ équivaut à : $n \geq 3$. D'autre part, on sait que :

$$\underbrace{q_m \frac{a}{p}} < \frac{a}{p} \quad \text{si } m \text{ est pair et } m > 0 ,$$

et

$$\underbrace{q_{n-1} \frac{a}{p}} = \begin{cases} \frac{1}{p} & \text{si } n-1 \text{ est pair} \\ \frac{p-1}{p} & \text{si } n-1 \text{ est impair} . \end{cases}$$

Il existe un entier k et un seul, $1 \leq k \leq p-2$ tel que :

$$\underbrace{(k+1) \frac{a}{p}} = \frac{p-1}{p} ;$$

il est donné par : $k+1 = \begin{cases} q_{n-1} & \text{si } n \text{ est pair} \\ p - q_{n-1} & \text{si } n \text{ est impair} \end{cases}$. On vérifie que $k > 1$.

Montrons qu'il existe un entier i , $1 \leq i < k$ tel que :

$$\underbrace{(i+1) \frac{a}{p}} < \frac{a}{p} .$$

Si n est impair, prenons $i+1 = q_{n-1}$; on a : $\underbrace{q_{n-1} \frac{a}{p}} = \frac{1}{p} < \frac{a}{p}$.

Si n est pair : $n-2 \geq 2$, prenons alors : $i+1 = q_{n-2}$; on a $\underbrace{q_{n-2} \frac{a}{p}} < \frac{a}{p}$.

Le couple (i, j) avec $j = k-i$ répond à la question, en effet $i+j = k < p-1$ et comme $\underbrace{(j+1) \frac{a}{p}} < \underbrace{(k+1) \frac{a}{p}} = \frac{p-1}{p}$ il satisfait à l'inégalité (1) .

3. DETERMINATION DE L'ORDRE ASSOCIE, $\mathfrak{D}$.

Proposition 3.

On suppose $t \geq 1$.

L'ordre $\mathfrak{D}$, est le sous A-module de $k[G]$ engendré par la famille :

$(\frac{f^i}{n_i})_{\overline{w}}^{0 \leq i \leq p-1}$, où les entiers n_i , pour $0 \leq i \leq p-1$, sont donnés par :

$$n_i = ia_0 + \min_{0 \leq j \leq p-1-i} ([(i+j+1)\frac{a}{p}] - [(j+1)\frac{a}{p}]) .$$

Démonstration de la proposition 3 :

1) Si a est différent de zéro, nous allons déterminer $\mathfrak{D}$, en écrivant que $\mathfrak{D}$ est inclus dans $\mathfrak{U}_\theta$ et que $\mathfrak{D}$ est l'ordre associé à gauche à $\mathfrak{U}_\theta$ (proposition 1 du chapitre I).

Soit $\mathfrak{D}'$ le sous A-module de $k[G]$ engendré par la famille $(\frac{f^i}{n_i})_{\overline{w}}^{0 \leq i \leq p-1}$, où les entiers n_i sont pour tout i , $0 \leq i \leq p-1$, les plus grands entiers vérifiant : $\frac{f^i}{n_i} \mathfrak{U}_\theta \subset \mathfrak{U}_\theta$.

D'après la proposition 1 du chapitre I, $\mathfrak{D}'$ est inclus dans $\mathfrak{D}$. Nous allons tout d'abord déterminer les entiers n_i ($0 \leq i \leq p-1$) puis montrer que : $\mathfrak{D} = \mathfrak{D}'$.

a) Un raisonnement analogue à celui du lemme 2 de ce chapitre, montre que pour tout i , $0 \leq i \leq p-1$, n_i est le plus grand entier vérifiant les inégalités :

$$(1') \quad \text{si } 0 \leq j \leq p-1-i \quad n_i + v_j \leq v_{i+j}$$

$$(2') \quad \text{si } j > p-1-i \quad n_i + v_j \leq e_0 + v_{i+j+1-p} .$$

D'après le lemme 3 on a toujours pour $j > p-1-i$:

$$v_i + v_j \leq e_0 + v_{i+j+1-p} ;$$

les inégalités (1') donnant pour $j = 0$, $n_i \leq v_i$, les inégalités (2') sont automatiquement vérifiées.

On peut alors écrire : $n_i = \min_{0 \leq j \leq p-1-i} (v_{i+j} - v_j)$ pour $0 \leq i \leq p-1$

d'où $n_i = ia_0 + \min_{0 \leq j \leq p-1-i} ([(i+j+1)\frac{a}{p}] - [(j+1)\frac{a}{p}])$.

Remarquons que pour tout i , $1 \leq i \leq p-1$, on a : $v_{i-1} \leq n_i \leq v_i$. En effet, l'entier v_{i-1} vérifie les conditions (1') et (2'). On a de plus $n_0 = 0 = v_0$ et $n_{p-1} = v_{p-1} = (p-1)a_0 + a$.

b) Montrons que : $\mathfrak{D} \subset \mathfrak{D}'$.

Un élément α de $\mathfrak{D}$ peut s'écrire :

$$\alpha = \sum_{i=0}^{p-1} a_i \frac{f^i}{\overline{n_i}} \quad \text{avec pour tout } i, a_i \text{ dans } k.$$

D'après la remarque précédente : a_0 et a_{p-1} sont dans A et pour $1 \leq i \leq p-2$, $\overline{a_i}$ est dans A . Notons i_0 , le plus grand entier compris entre 1 et $p-2$, tel que le coefficient a_{i_0} ne soit pas dans A .

$$\alpha' = \sum_{i=1}^{i_0} a_i \frac{f^i}{\overline{n_i}}$$

est encore un élément de $\mathfrak{D}$ et nous savons que : $n_{i_0} = v_{i_0} - 1$. Il existe donc un entier j_0 , tel que $i_0 + j_0 \leq p-1$ et $v_{i_0} + v_{j_0} > v_{i_0 + j_0} = n_{i_0 + j_0}$.

D'après la proposition 1, c) du chapitre I :

$$\alpha' \frac{f^{j_0}}{\overline{v_{j_0}}} \quad \text{est un élément de } \mathfrak{D}.$$

$$\alpha' \frac{f^{j_0}}{\overline{v_{j_0}}} = \sum_{i=1}^{i_0-1} a_i \frac{f^{i+j_0}}{\overline{n_{i+j_0}}} + a_{i_0} \frac{f^{i_0+j_0}}{\overline{v_{i_0+j_0}}};$$

comme pour i , $1 \leq i \leq i_0-1$, on a : $i+j_0 < i_0+j_0 \leq p-1$, le coefficient a_{i_0} est nécessairement dans A . Il y a contradiction avec l'hypothèse, on en déduit que pour i , $0 \leq i \leq p-1$, a_i est dans A et par conséquent α est dans $\mathfrak{D}'$.

2) Si a est nul, d'après la proposition 1, b) de ce chapitre on sait que : $\mathfrak{D} = \mathfrak{D}_m$ et que $\mathfrak{D}_m$ est le sous A -module de $k[G]$ engendré par la famille $(1)_{\chi_i, 0 \leq i \leq p-1}$.

La formule de la proposition 3 donne pour $a = 0$

$$n_i = ia_0 = i \frac{e_0}{p-1},$$

pour $0 \leq i \leq p-1$, puisque dans ce cas $t = \frac{pe_0}{p-1}$.

On peut alors vérifier directement que $\mathfrak{D} = \mathfrak{D}_m$ est le sous A-module de $k[G]$ engendré par la famille $\left(\frac{f^i}{ie_0} \right)_{\substack{p-1 \\ 0 \leq i \leq p-1}}$ (cf. lemme 6 de ce chapitre). Il suffit de vérifier que $\left(\frac{f^i}{ie_0} \right)_{\substack{p-1 \\ 0 \leq i \leq p-1}}$ est une base de $\mathfrak{D}_m$, en montrant que le déterminant de la matrice de passage de la famille $(1_{\chi_i})_{0 \leq i \leq p-1}$ à la famille $\left(\frac{f^i}{ie_0} \right)_{\substack{p-1 \\ 0 \leq i \leq p-1}}$, est une unité.

Remarque.

On voit que l'idempotent, $\frac{1}{p} \sum_{i=0}^{p-1} \sigma^i$, de $k[G]$, appartient à $\mathfrak{D}$ si et seulement si, l'inégalité $e_0 \leq n_{p-1}$ est vérifiée ; en effet, on a

$$\sum_{i=0}^{p-1} \sigma^i = f^{p-1} + pf^{p-2} + \binom{p}{2} f^{p-3} + \dots + pf.$$

Ceci montre que, $\frac{1}{p} \sum_{i=0}^{p-1} \sigma^i$ appartient à $\mathfrak{D}$ si et seulement si :

$$(I) \quad \frac{pe_0}{p-1} - 1 \leq t \leq \frac{pe_0}{p-1}$$

(cf. la définition d'indice de ramification "presque maximal" [5]).

4. ETUDE DU $\mathfrak{D}$ -MODULE B DANS LE CAS OU : $t < \frac{pe_0}{p-1} - 1$

4.1. Proposition 4 .

Si $1 \leq t < \frac{pe_0}{p-1} - 1$, a non nul et a ne divise pas $p-1$, alors $\mathfrak{U}_\theta$ n'est pas un idéal principal de $\mathfrak{D}$.

Démonstration de la proposition 4 :

Soit α , un élément de $\mathfrak{U}_\theta$, on considère l'application A-linéaire,

ψ_α de $\mathfrak{D}$ dans $\mathfrak{U}_\theta$ définie par :

$$\psi_\alpha(\lambda) = \lambda\alpha \quad , \text{ pour tout } \lambda \text{ de } \mathfrak{D} .$$

On note, $M(\alpha)$, la matrice associée à cette application dans les bases respectives $\left(\frac{f^i}{n_i}\right)_{0 \leq i \leq p-1}$ et $\left(\frac{f^i}{v_i}\right)_{0 \leq i \leq p-1}$ de $\mathfrak{D}$ et de $\mathfrak{U}_\theta$. Les coefficients de $M(\alpha)$ sont dans A , on les désigne par μ_{ji} , j et i étant des entiers compris entre zéro et $p-1$.

α est un générateur de l'idéal à gauche $\mathfrak{U}_\theta$ de $\mathfrak{D}$ si, et seulement si, le déterminant de $M(\alpha)$ est une unité de A .

Dans les conditions de la proposition 4, nous allons montrer que pour tout α de $\mathfrak{U}_\theta$, le déterminant de $M(\alpha)$ est congru à zéro modulo l'idéal $\mathfrak{w}A$ de A , et que, par conséquent $\mathfrak{U}_\theta$ n'est pas un idéal principal de $\mathfrak{D}$.

Montrons tout d'abord que si α est un générateur de l'idéal $\mathfrak{U}_\theta$, on peut écrire : $\alpha = 1 + \sum_{i=1}^{p-1} b_i \frac{f^i}{v_i}$ avec b_i dans A pour $1 \leq i \leq p-1$. En effet, si $\mathfrak{U}_\theta = \mathfrak{D}\alpha$, α est un élément inversible de $k[G]$ dont l'inverse α' est dans $\mathfrak{D}$. On a : $\alpha = \sum_{i=0}^{p-1} a_i \frac{f^i}{v_i}$ avec a_i dans A , $\alpha' = \sum_{i=0}^{p-1} a'_i \frac{f^i}{n_i}$ avec a'_i dans A et $\alpha'\alpha = 1$. Par suite $a'_0 a_0 = 1$ et $a'_0 \alpha$ est encore un générateur de $\mathfrak{U}_\theta$ qui s'écrit :

$$a'_0 \alpha = 1 + \sum_{i=1}^{p-1} b_i \frac{f^i}{v_i} \quad \text{où } b_i = a'_0 a_i \text{ est dans } A .$$

Soit $\bar{\mu}$, l'image dans le corps résiduel $\bar{k} = A/\mathfrak{w}A$, d'un élément μ de A et soit $\overline{M(\alpha)}$ la matrice, dans $\bar{k}$, dont les coefficients sont $\bar{\mu}_{ji}$ pour i et j compris entre zéro et $p-1$.

Soit un entier i fixé, $0 \leq i \leq p-1$; pour tout entier k , $1 \leq k \leq p-1$ tel que : $i+k \geq p$, on exprime f^{i+k} comme combinaison linéaire des f^j , $1 \leq j \leq p-1$ [Chap.II, lemme 2] .

Si $1 \leq j < i$ on a : $\bar{\mu}_{ji} = 0$. En effet, d'après le lemme 3 a) de ce chapitre, pour k , $1 \leq k \leq p-1$ tel que $i+k \geq p$, on a :

$v_i + v_k \leq a + (p-1)a_o + v_{i+k+1-p}$. Or l'inégalité : $t < \frac{pe_o}{p-1} - 1$ entraîne que :
 $a + (p-1)a_o < e_o$, par suite pour $i+k \geq p$ on a $n_i + v_k < e_o + v_{i+k+1-p}$.
 Si l'on exprime $\frac{f^{i+k}}{n_i + v_k}$ dans la base $(\frac{f^j}{v_j})$ de $\mathfrak{U}_\theta$, les coefficients
 sont dans l'idéal $\mathfrak{p}A$.

D'autre part, $\overline{\mu_{ii}} = 1$ ou 0 suivant que : $n_i = v_i$ ou $n_i = v_i - 1$.
 La matrice $\overline{M(\alpha)}$ est donc une matrice triangulaire et son déterminant s'écrit :

$$\det \overline{M(\alpha)} = \prod_{i=0}^{p-1} \overline{\mu_{ii}}.$$

Si a est non nul et si a ne divise pas $p-1$, d'après la proposition 2, $\mathfrak{U}_\theta$ est différent de $\mathfrak{D}$ et par suite il existe au moins un entier i , $1 \leq i \leq p-2$, tel que $n_i = v_i - 1$. Dans ces conditions, nous obtenons $\det \overline{M(\alpha)} = 0$. Ceci achève la démonstration de la proposition 4.

4.2. On peut résumer l'ensemble des résultats obtenus par le théorème suivant :

Théorème 1.

Si $t \equiv 0$ (modulo p) B est un $\mathfrak{D}$ -module libre.

Si $t \not\equiv 0$ (modulo p) et si $t < \frac{pe_o}{p-1} - 1$, pour que B soit un $\mathfrak{D}$ -module libre, il faut et il suffit que a divise $p-1$.

Démonstration du théorème :

La proposition 2 permet d'obtenir le résultat suivant : si $t \equiv 0 \pmod{p}$ B est un $\mathfrak{D}$ -module libre, si $t \not\equiv 0 \pmod{p}$ et si a divise $p-1$, B est un $\mathfrak{D}$ -module libre.

La proposition 2 du chapitre I et les propositions 2 et 4 du chapitre II permettent de dire que : si a est non nul, si a ne divise pas $p-1$ et si $t < \frac{pe_o}{p-1} - 1$, B n'est pas un $\mathfrak{D}$ -module libre.

Exemple : Si $k = \mathbb{Q}_p$ et si K/k est une extension cyclique de degré p , on a toujours $t = 1$ et B est un $\mathfrak{D}$ -module libre. Ce résultat se déduit du résultat de [6].

4.3. On peut déduire du théorème précédent les deux corollaires suivants :

Corollaire 1.

Si t vérifie les conditions : $t \not\equiv 0 \pmod{p}$, $t < \frac{pe_0}{p-1}$ et si a ne divise pas $p-1$, alors B n'est pas un $\mathfrak{O}$ -module projectif.

Démonstration :

A étant un anneau local, $\mathfrak{O}$ est un anneau semi-local. Puisque G est un groupe cyclique et d'après la proposition 3 du chapitre I, B est $\mathfrak{O}$ -libre si et seulement si B est un $\mathfrak{O}$ -module projectif.

Ce corollaire donne un exemple d'extension K/k telle que B ne soit pas projectif sur $\mathfrak{O}$ et apporte ainsi une réponse à la question posée dans [9] §4 .

Exemple 1 : Soit $k = \mathbb{Q}_5(5^{1/4})$ et soit K le corps de décomposition sur k du polynôme : $X^5 - 5X - 5^{1/2}$; l'extension K/k est cyclique de degré 5 , et son nombre de ramification est $t = a = 3$ d'après [12] Ch.IV §2 exercice 5 ; on en déduit que B n'est pas un $\mathfrak{O}$ -module projectif.

Corollaire 2.

Soit K/k une extension cyclique de degré p , de corps de nombres, vérifiant les conditions du paragraphe 3 du chapitre I. On note t le nombre de ramification de l'extension $K_{\mathfrak{p}}/k_{\mathfrak{p}}$, et a le reste de t modulo p . Si $t \not\equiv 0 \pmod{p}$, $t < \frac{pe_0}{p-1} - 1$ et a ne divise pas $p-1$, B n'est pas un $\mathfrak{O}$ -module projectif.

Démonstration :

$B_{\mathfrak{p}}$, anneau des entiers de $K_{\mathfrak{p}}$, n'est pas un $\tilde{\mathfrak{O}}$ -module projectif d'après le corollaire 1 ; on déduit alors de la proposition 5 du chapitre I que B n'est pas un $\mathfrak{O}$ -module projectif.

Exemple 2 : Si $k = \mathbb{Q}(5^{1/4})$, si K est le corps de décomposition sur k du polynôme : $X^5 - 5X - 5^{1/2}$, l'extension K/k est cyclique de degré 5 , son nombre de ramification t est 3 . Nous sommes dans les conditions du para-

graphe 3 du chapitre I . $B_{\mathfrak{p}}$ n'est pas projectif sur $\tilde{\mathfrak{O}}$ d'après l'exemple 1 ci-dessus, B n'est donc pas un $\mathfrak{O}$ -module projectif.

4.4. Dans le cas où l'indice de ramification t vérifie la double inégalité (I) de la remarque du paragraphe 3 de ce chapitre, les résultats ci-dessus ne permettent pas de conclure lorsque a est non nul et que a ne divise pas $p-1$. Ce dernier cas fera l'objet du paragraphe 5.

5. CAS OU L'INDICE DE RAMIFICATION t EST "PRESQUE MAXIMAL".

Dans ce paragraphe, le nombre de ramification t est supérieur ou égal à 1 et vérifie l'inégalité :

$$(I) \quad \frac{pe_{\mathfrak{O}}}{p-1} - 1 \leq t \leq \frac{pe_{\mathfrak{O}}}{p-1} \quad [\S 3 \text{ chapitre II, remarque}] .$$

Remarquons que l'inégalité (I) entraîne : $e_{\mathfrak{O}} = a_{\mathfrak{O}}(p-1) + a$.

5.1. Suite des parties fractionnaires des multiples de $\frac{t}{p}$.

Dans la détermination de l'ordre $\mathfrak{O}$, (proposition 3, ch.II), intervient une suite finie d'entiers n_i ($0 \leq i \leq p-1$) .

Nous allons donner une autre expression de la suite (n_i) en faisant intervenir les minima successifs de la suite des parties fractionnaires des multiples de $\frac{t}{p}$. Rappelons les notations suivantes : $\frac{t}{p} = a_{\mathfrak{O}} + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots}}}$ = $[a_{\mathfrak{O}}, a_1, \dots, a_n]$ avec $a_n > 1$ le développement de $\frac{t}{p}$ en fraction continue ; $q_{\mathfrak{O}} = 1$, $q_1 = a_1$, $\dots$, $q_i = a_i q_{i-1} + q_{i-2}$, $\dots$, $q_n = p$ les dénominateurs des "réduites" successives de $\frac{t}{p}$; cf (paragraphe 2 de ce chapitre).

Soit E , l'ensemble des entiers h tels que $1 \leq h < p$ et vérifiant la condition : "pour tout entier h' , tel que $1 \leq h' < h$, on a $\sqrt{h' \frac{t}{p}} > \sqrt{h \frac{t}{p}}$ " .

Lemme 4.

Si $n \geq 2$, l'ensemble E est l'ensemble des entiers $a'_{2i+2} q_{2i+1} + q_{2i}$
où $0 \leq i < \frac{n-1}{2}$ et où :

$$0 \leq a'_{2i+2} < a_{2i+2} \quad \text{si} \quad i \neq \frac{n-3}{2}$$

$$0 \leq a'_{2i+2} \leq a_{2i+2} \quad \text{si} \quad i = \frac{n-3}{2}$$

Démonstration :

Notons $\|x\|$ la distance à l'entier le plus proche du nombre réel x .
On sait que les minima successifs de la suite $\|h \frac{t}{p}\|$ ($0 \leq h \leq p-1$) sont
égaux à : $\delta_i = \|q_i \frac{t}{p}\| = \|q_i \frac{a}{p}\|$ ($0 \leq i \leq n-1$).

Considérons un cercle (C) orienté de longueur 1 et fixons sur ce cercle une
origine O des abscisses. On note M_i le point du cercle tel que :

$$\overrightarrow{OM_i} = i \frac{t}{p} = i \frac{a}{p}.$$

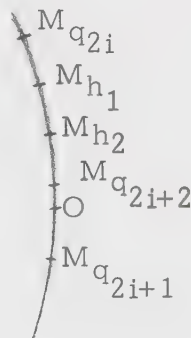
$$- \text{ si } i \text{ est pair : } \underbrace{q_i \frac{a}{p}} < \frac{1}{2} \quad \text{et} \quad \delta_i = \underbrace{q_i \frac{a}{p}};$$

$$- \text{ si } i \text{ est impair : } \underbrace{q_i \frac{a}{p}} > \frac{1}{2} \quad \text{et} \quad 1 - \delta_i = \underbrace{q_i \frac{a}{p}}.$$

On en déduit que si j est pair, $0 \leq j \leq n-1$, q_j appartient à E .

Remarquons que si h et k sont deux entiers tels que $|h-k| < q_i$, $1 \leq i \leq n-1$
alors $\|(h-k) \frac{a}{p}\| \geq \delta_{i-1}$, c'est-à-dire que le plus petit arc joignant M_h et
 M_k est de longueur supérieure ou égale à δ_{i-1} .

Les points $M_{q_{2i}}$, $M_{q_{2i+1}}$, $M_{q_{2i+2}}$, pour $0 \leq i \leq \frac{n-3}{2}$ sont donc
disposés de la manière suivante sur (C) :



Cherchons quels sont les entiers h de E compris entre q_{2i} et q_{2i+2} pour
 $0 \leq i < \frac{n-1}{2}$.

a) Cherchons tout d'abord quels sont les points M_h , $q_{2i} < h < q_{2i+2}$, qui sont sur le cercle (C) entre les points $M_{q_{2i+2}}$ et $M_{q_{2i}}$.

- si $a_{2i+2} > 1$ soit $h_1 = q_{2i+1} + q_{2i}$, M_{h_1} se trouve entre $M_{q_{2i+2}}$ et $M_{q_{2i}}$. En effet $\underbrace{h_1}_{\frac{a}{p}} = \underbrace{q_{2i+1}}_{\frac{a}{p}} + \underbrace{q_{2i}}_{\frac{a}{p}} - 1 < \underbrace{q_{2i}}_{\frac{a}{p}}$, et $\underbrace{h_1}_{\frac{a}{p}} > \underbrace{q_{2i+2}}_{\frac{a}{p}}$ car $h_1 < q_{2i+2}$. De plus $\|(h_1 - q_{2i})_{\frac{a}{p}}\| = \delta_{2i+1}$.

- si $a_{2i+2} > 2$ soit $h_2 = 2q_{2i+1} + q_{2i}$, M_{h_2} se trouve entre $M_{q_{2i+2}}$ et M_{h_1} . En effet $\underbrace{h_2}_{\frac{a}{p}} = \underbrace{q_{2i+1}}_{\frac{a}{p}} + \underbrace{h_1}_{\frac{a}{p}} - 1 < \underbrace{h_1}_{\frac{a}{p}}$, et comme $h_2 < q_{2i+2}$, $\underbrace{h_2}_{\frac{a}{p}} > \underbrace{q_{2i+2}}_{\frac{a}{p}}$. De plus $\|(h_2 - h_1)_{\frac{a}{p}}\| = \delta_{2i+1}$.

Par récurrence :

- si $a_{2i+2} > a'_{2i+2} \geq 1$ soit $h = a'_{2i+2}q_{2i+1} + q_{2i}$ et $h' = (a'_{2i+2} - 1)q_{2i+1} + q_{2i}$, M_h se trouve entre $M_{q_{2i+2}}$ et $M_{h'}$. En effet $\underbrace{h}_{\frac{a}{p}} = \underbrace{q_{2i+1}}_{\frac{a}{p}} + \underbrace{h'}_{\frac{a}{p}} - 1 < \underbrace{h'}_{\frac{a}{p}}$, et $\underbrace{h}_{\frac{a}{p}} > \underbrace{q_{2i+2}}_{\frac{a}{p}}$. De plus $\|(h - h')_{\frac{a}{p}}\| = \delta_{2i+1}$.

Les points M_h , où $h = a'_{2i+2}q_{2i+1} + q_{2i}$, $0 < a'_{2i+2} < a_{2i+2}$ sont donc sur le cercle (C) entre $M_{q_{2i+2}}$ et $M_{q_{2i}}$.

Soit M_k , $q_{2i} < k < q_{2i+2}$, un point de (C) entre $M_{q_{2i+2}}$ et $M_{q_{2i}}$. Il existe alors $h = xq_{2i+1} + q_{2i}$, $0 \leq x \leq a_{2i+2}$ tel que : $\|(h - k)_{\frac{a}{p}}\| < S_{2i+1}$ comme $|h - k| < q_{2i+2}$ c'est que $h = k$.

On en déduit que si : $h < q_{2i+2}$, les seuls points M_h de (C) compris entre $M_{q_{2i+2}}$ et $M_{q_{2i}}$ sont les $M_{a'_{2i+2}q_{2i+1} + q_{2i}}$ avec $0 < a'_{2i+2} < a_{2i+2}$.

b) Les entiers $h = a'_{2i+2}q_{2i+1} + q_{2i}$, $0 < a'_{2i+2} < a_{2i+2}$ sont dans E.

En effet, supposons que $h' < h$ et $\underbrace{h' \frac{a}{p}} < \underbrace{h \frac{a}{p}}$. Le point $M_{h'}$ est entre les points $M_{q_{2i+2}}$ et $M_{q_{2i}}$; comme $\underbrace{h'} < \underbrace{q_{2i+2}}$ on a : $h' = xq_{2i+1} + q_{2i}$ avec $0 \leq x < a_{2i+2}$. Mais alors si $\underbrace{h' \frac{a}{p}} < \underbrace{h \frac{a}{p}}$ c'est que $h' > h$. On voit donc, si $h' < h$, que : $\underbrace{h' \frac{a}{p}} > \underbrace{h \frac{a}{p}}$.

c) Les entiers $h = a'_{2i+2}q_{2i+1} + q_{2i}$, $0 < a'_{2i+2} < a_{2i+2}$, sont les seuls entiers de E compris entre q_{2i} et q_{2i+2} ; en effet les points M_h correspondants sont les seuls points de (C) , avec $q_{2i} < h < q_{2i+2}$, qui soient entre $M_{q_{2i+2}}$ et $M_{q_{2i}}$.

Proposition 5.

Soit (n_i) , $0 \leq i \leq p-1$, la suite d'entiers définie par :

$$n_i = ia_o + \min_{0 \leq j \leq p-1-i} ([(i+j+1) \frac{a}{p}] - [(j+1) \frac{a}{p}])$$

on a : $n_i = ia_o + [i \frac{a}{p}]$ si $p-i$ n'appartient pas à E ;

$n_i = ia_o + [i \frac{a}{p}] + 1$ si $p-i$ appartient à E .

Démonstration de la proposition 5 :

Ecrivons pour un entier i fixé $0 \leq i \leq p-1$ et $0 \leq j < p-1-i$:

$$(i+j+1) \frac{a}{p} - (j+1) \frac{a}{p} = [(i+j+1) \frac{a}{p}] - [(j+1) \frac{a}{p}] + \underbrace{(i+j+1) \frac{a}{p}} - \underbrace{(j+1) \frac{a}{p}} = [i \frac{a}{p}] + \underbrace{i \frac{a}{p}} ;$$

nous voyons que $[(i+j+1) \frac{a}{p}] - [(j+1) \frac{a}{p}] = [i \frac{a}{p}] + \underbrace{i \frac{a}{p}} + \underbrace{(j+1) \frac{a}{p}} - \underbrace{(i+j+1) \frac{a}{p}}$ ou

$$\text{encore } [(i+j+1) \frac{a}{p}] - [(j+1) \frac{a}{p}] = \begin{cases} [i \frac{a}{p}] + 1 & \text{si } \underbrace{i \frac{a}{p}} + \underbrace{(j+1) \frac{a}{p}} > 1 \\ [i \frac{a}{p}] + 0 & \text{si } \underbrace{i \frac{a}{p}} + \underbrace{(j+1) \frac{a}{p}} < 1 \end{cases}.$$

Posons $i = p-h$, alors :

$$n_i = ia_o + [i \frac{a}{p}] + 1 \text{ si pour tout } j \text{ tel que } 1 \leq j+1 < h ; \underbrace{(j+1) \frac{a}{p}} > \underbrace{h \frac{a}{p}}.$$

$$n_i = ia_o + [i \frac{a}{p}] + 0 \text{ s'il existe } j, 1 \leq j+1 < h \text{ tel que } \underbrace{(j+1) \frac{a}{p}} < \underbrace{h \frac{a}{p}}$$

ce qui démontre la proposition 5.

5.2. Etude du $\mathfrak{D}$ -module B dans le cas où t est "presque maximal".

5.2.1. Soit un entier J , $0 \leq J \leq p-1$, fixé, et l'élément $\frac{f^J}{\mathfrak{w} \nu_J}$ de $\mathfrak{U}_\theta$.

On considère, comme dans la démonstration de la proposition 4 de ce chapitre, l'application A -linéaire de $\mathfrak{D}$ dans $\mathfrak{U}_\theta$ définie par :

$\lambda \rightarrow \lambda \frac{f^J}{\mathfrak{w} \nu_J}$ où λ est dans $\mathfrak{D}$. On note $M(\frac{f^J}{\mathfrak{w} \nu_J})$ la matrice associée à cette application linéaire dans les bases respectives $(\frac{f^1}{n_1})$ et $(\frac{f^j}{\mathfrak{w} \nu_j})$ de $\mathfrak{D}$ et de $\mathfrak{U}_\theta$. On désigne par $\mu_{j,i}^{(J)}$, $(0 \leq j, i \leq p-1)$ les coefficients de cette matrice, coefficients qui appartiennent à A .

Si μ est un élément de A , on note $\bar{\mu}$ son image dans le corps résiduel $\bar{k} = A/\mathfrak{w}A$.

On note d_j ($0 \leq j \leq p-1$) le plus grand entier d tel que : $\nu_{j+d} = \nu_j$; on remarque que : $0 \leq d_j \leq a_1+1$ et que si $a_0 \neq 0$, $d_j = 0$ pour tout j .

La matrice $M(1)$ est diagonale et $\bar{\mu}_{ii}^{(0)}$ vaut 1 ou 0 suivant que $n_i = \nu_i$ ou que $n_i = \nu_{i-1}$.

Lorsque J est supérieur ou égal à 1, on a le résultat suivant :

Lemme 5.

Soit J un entier tel que : $1 \leq J \leq p-1$. On suppose que l'entier i vérifie : $0 \leq i \leq p-1$ et on pose $i = p-h$.

a) Dans le cas où : $h \geq J+1$, nous avons :

si $j \neq J+i$: $\bar{\mu}_{j,i}^{(J)} = 0$;

si h n'appartient pas à E : $\bar{\mu}_{J+i,i}^{(J)} = \begin{cases} 1 & \text{si } h = p \\ 1 & \text{si } (J+1)\frac{a}{p} < h\frac{a}{p} \\ 0 & \text{sinon} \end{cases}$;

si h appartient à E : $\bar{\mu}_{J+i,i}^{(J)} = 1$.

b) Dans le cas où : $h < J+1$, nous avons en posant, $m = J+1-h$:

si $j < m$ ou si $j > m+dm$: $\bar{\mu}_{j,i}^{(J)} = 0$;

si $m \leq j \leq m+d$ et si h n'appartient pas à E : $\begin{cases} \bar{\mu}_{j,i}^{(J)} \neq 0 & \text{si } \frac{a}{p} + (J+1)\frac{a}{p} < \frac{h\frac{a}{p}}{p}; \\ \bar{\mu}_{j,i}^{(J)} = 0 & \text{sinon} \end{cases}$

si $m \leq j \leq m+d_m$ et si h appartient à E : $\begin{cases} \bar{\mu}_{j,i}^{(J)} \neq 0 & \text{si } \frac{a}{p} + (J+1)\frac{a}{p} < \frac{h\frac{a}{p}}{p} + 1 \\ \bar{\mu}_{j,i}^{(J)} = 0 & \text{sinon.} \end{cases}$

Démonstration :

a) Cas où $h \geq J+1$ (c'est-à-dire $i+J \leq p-1$) . Dans ce cas $\frac{f^{i+J}}{n_i + v_J}$ se décompose sur $\frac{f^{i+J}}{v_{i+J}}$ on a donc $\bar{\mu}_{j,i}^{(J)} = 0$ si j est différent de $J+i$.

D'autre part, écrivons $n_i + v_J = (i+J)a_0 + [i\frac{a}{p}] + [(J+1)\frac{a}{p}] + \epsilon$, où $\epsilon = 0$ si h n'est pas dans E , $\epsilon = 1$ si h est dans E et

$$v_{i+J} = (i+J)a_0 + [(i+J+1)\frac{a}{p}] .$$

Comme $[(i+J+1)\frac{a}{p}] - [i\frac{a}{p}] - [(J+1)\frac{a}{p}] = \frac{i\frac{a}{p}}{p} + (J+1)\frac{a}{p} - (i+J+1)\frac{a}{p}$, on a :

$$v_{i+J}^{-n_i - v_J} = \frac{i\frac{a}{p}}{p} + (J+1)\frac{a}{p} - (i+J+1)\frac{a}{p} - \epsilon \quad \text{où} \quad \begin{cases} \epsilon = 0 & \text{si } h \text{ n'est pas dans } E \\ \epsilon = 1 & \text{si } h \text{ est dans } E . \end{cases}$$

On en déduit que :

- si h n'est pas dans E :

. pour $h = p$: $\bar{\mu}_{J+i,i}^{(J)} = 1$;

. pour $h \neq p$ comme ϵ est nul, $v_{i+J}^{-n_i - v_J} = 0$ si

et seulement si $(J+1)\frac{a}{p} < \frac{h\frac{a}{p}}{p}$

donc : $\bar{\mu}_{J+i,i}^{(J)} = 1$ si $(J+1)\frac{a}{p} < \frac{h\frac{a}{p}}{p}$ et $\bar{\mu}_{J+i,i}^{(J)} = 0$ sinon.

- si h est dans E , et si $J+1 \leq h$ par définition de E ,

$$(J+1)\frac{a}{p} \geq \frac{h\frac{a}{p}}{p} ,$$

donc

$$\bar{\mu}_{J+i,i}^{(J)} = 1 .$$

b) Cas où $h < J+1$. On pose $m = J+1-h$.

On a vu dans la démonstration du lemme 2 de ce chapitre que :

$$f^{p-1+m} = pr_{p-1}f^{p-1} + pr_{p-2}f^{p-2} + \dots + pr_m f^m + p^2 r_{m-1}f^{m-1} + \dots + p^2 r_1 f$$

où les r_i sont des unités de A . $\frac{f^{i+J}}{n_i + v_J}$ se décompose alors sur les $\frac{f^j}{v_j}$, $1 \leq j \leq p-1$. Rappelons que : $n_i + v_J \leq e_o + v_m$.

■ si $j < m$, $\mu_{j,i}^{(J)} = 0$.

■ si $j > m+dm$, on a : $v_j > v_m$ et par suite $\frac{p \bar{w}^{v_j}}{n_i + v_J}$ est dans l'idéal $\bar{w}A$ c'est-à-dire $\mu_{j,i}^{(J)} = 0$

■ si $m \leq j \leq m+d_m$ on a : $v_j = v_m$.

$$n_i + v_J = (i+J)a_o + [i \frac{a}{p}] + [(J+1)\frac{a}{p}] + \epsilon \quad \text{où} \quad \begin{cases} \epsilon = 0 & \text{si } h \text{ n'est pas dans } E \\ \epsilon = 1 & \text{si } h \text{ est dans } E \end{cases}$$

$$e_o + v_m = e_o + (i+J)a_o - (p-1)a_o + [(m+1)\frac{a}{p}]$$

comme

$$[(m+1)\frac{a}{p}] - [i \frac{a}{p}] - [(J+1)\frac{a}{p}] = -(p-1)\frac{a}{p} - \underbrace{(m+1)\frac{a}{p}} + \underbrace{i \frac{a}{p}} + \underbrace{(J+1)\frac{a}{p}}$$

on a

$$e_o + v_m - n_i - v_J = e_o - (p-1)a_o - (p-1)\frac{a}{p} - \underbrace{(m+1)\frac{a}{p}} + \underbrace{i \frac{a}{p}} + \underbrace{(J+1)\frac{a}{p}} - \epsilon$$

$$e_o + v_m - n_i - v_J = \frac{a}{p} - \underbrace{(m+1)\frac{a}{p}} + \underbrace{i \frac{a}{p}} + \underbrace{(J+1)\frac{a}{p}} - \epsilon$$

$$e_o + v_m - n_i - v_J = \frac{a}{p} - \underbrace{(J+2-h)\frac{a}{p}} + 1 - \underbrace{h \frac{a}{p}} + \underbrace{(J+1)\frac{a}{p}} - \epsilon$$

or $\frac{a}{p} + \underbrace{(J+1)\frac{a}{p}} - \underbrace{h \frac{a}{p}}$ est égal à : $\underbrace{(J+2-h)\frac{a}{p}}$ si $0 \leq \frac{a}{p} + \underbrace{(J+1)\frac{a}{p}} - \underbrace{h \frac{a}{p}} < 1$

$$\underbrace{(J+2-h)\frac{a}{p}} - 1 \quad \text{si} \quad -1 \leq \frac{a}{p} + \underbrace{(J+1)\frac{a}{p}} - \underbrace{h \frac{a}{p}} < 0$$

$$\underbrace{(J+2-h)\frac{a}{p}} + 1 \quad \text{si} \quad 1 \leq \frac{a}{p} + \underbrace{(J+1)\frac{a}{p}} - \underbrace{h \frac{a}{p}} < 2.$$

- Si h n'appartient pas à E , $\epsilon = 0$, donc :

$$e_o + v_m = n_i + v_J \quad \text{si et seulement si} \quad \frac{a}{p} + \underbrace{(J+1)\frac{a}{p}} < \underbrace{h \frac{a}{p}}$$

c'est-à-dire que :

$$\mu_{j,i}^{(J)} \neq 0 \quad \text{si} \quad \frac{a}{p} + \underbrace{(J+1)\frac{a}{p}} < \underbrace{h \frac{a}{p}}$$

et

$$\mu_{j,i}^{(J)} = 0 \quad \text{sinon.}$$

- Si h est dans E , $\epsilon = 1$, donc :

$e_o + v_m = n_i + v_J$ si et seulement si $\frac{a}{p} + \underbrace{(J+1)\frac{a}{p}} < \underbrace{h\frac{a}{p}} + 1$
c'est-à-dire que :

$$\underline{\mu_{j,i}^{(j)} \neq 0 \quad \text{si} \quad \frac{a}{p} + \underbrace{(J+1)\frac{a}{p}} < \underbrace{h\frac{a}{p}} + 1}$$

$$\underline{\mu_{j,i}^{(j)} = 0 \quad \text{sinon} .}$$

Ceci termine la démonstration du lemme 5.

5.2.2. Soit $\alpha = \sum_{J=0}^{p-1} x_J \frac{f^J}{v_J}$ un élément de l'idéal $\mathfrak{u}_\theta$; $M(\alpha)$ est la matrice associée à l'application A -linéaire de $\mathfrak{D}$ dans $\mathfrak{u}_\theta$ définie par :

$\lambda \mapsto \lambda\alpha$. On peut écrire $M(\alpha) = \sum_{J=0}^{p-1} x_J M(\frac{f^J}{v_J})$. Rappelons que α n'est générateur de l'idéal $\mathfrak{u}_\theta$ de $\mathfrak{D}$ que si le déterminant de $M(\alpha)$ est une unité de A .

L'idéal $\mathfrak{u}_\theta$ est donc un idéal principal de l'anneau $\mathfrak{D}$ si, et seulement si, il existe un élément α de $\mathfrak{u}_\theta$ tel que le déterminant de $M(\alpha)$ soit une unité de A .

Les deux propositions suivantes (propositions 6 et 7) vont permettre de conclure dans tous les cas, en déterminant à quelles conditions $\mathfrak{u}_\theta$ est un idéal principal de $\mathfrak{D}$.

Proposition 6.

Si l'entier n est inférieur ou égal à 4 , $\mathfrak{u}_\theta$ est un idéal à gauche principal de $\mathfrak{D}$.

Démonstration de la proposition 6 :

L'hypothèse " $n \leq 2$ " est équivalente à l'hypothèse " $a = 0$ ou a divise $p-1$ " . Dans ce cas nous savons que $\mathfrak{u}_\theta = \mathfrak{D}$ (proposition 2 de ce chapitre) et donc que $\mathfrak{u}_\theta$ est un idéal principal de $\mathfrak{D}$.

Il nous reste à traiter les cas $n = 3$ et $n = 4$.

Soit $J = q_2 - 1$ et $\alpha = u + \frac{f^J}{v_J}$ où u est une unité de A . On a :

$$M(\alpha) = uM(1) + M\left(\frac{f^J}{\overline{v}_J}\right) .$$

Cas $n = 3$.

L'ensemble E est donné par :

$$E = \{1, q_1+1, 2q_1+1, \dots, (a_2-1)q_1+1, q_2\} \quad (\text{cf } \S 5.1 \text{ du chapitre II}) .$$

Utilisons le lemme 5 pour étudier la matrice $M\left(\frac{f^J}{\overline{v}_J}\right)$.

Décrivons la i -ème colonne de $M\left(\frac{f^J}{\overline{v}_J}\right)$, $0 \leq i \leq p-1$; posons $h = p-i$.

■ Si $h \geq J+1 = q_2$: $\mu_{J+i,i}^{-(J)} = 1$ et $\mu_{j,i}^{-(J)} = 0$ pour j différent de $J+i$.

En effet, si h n'est pas dans E et si h est différent de p , on a toujours :

$$\underbrace{(J+1)\frac{a}{p}} = \underbrace{q_2\frac{a}{p}} = \frac{1}{p} < \underbrace{h\frac{a}{p}} \quad \text{car } p > h > q_2 .$$

■ Si $h < J+1$, c'est-à-dire $h \leq q_2-1$ posons $i+J = p-1+m$.

- Supposons h dans E . D'après la définition de E , q_2 étant dans E on a : $\underbrace{h\frac{a}{p}} > \underbrace{q_2\frac{a}{p}}$ et donc :

$$\underbrace{(J+1)\frac{a}{p}} + \frac{a}{p} = \underbrace{q_2\frac{a}{p}} + \frac{a}{p} = \frac{1}{p} + \frac{a}{p} < \underbrace{h\frac{a}{p}} + 1$$

on en déduit :

$$\mu_{j,i}^{-(J)} \neq 0 \quad \text{pour } m \leq j \leq m+d_m$$

d'autre part :

$$\mu_{j,i}^{-(J)} = 0 \quad \text{si } j < m \quad \text{ou } j > m+d_m .$$

- Supposons h non dans E . On a $\underbrace{h\frac{a}{p}} > \frac{a}{p}$, en effet si $\underbrace{h\frac{a}{p}} < \frac{a}{p}$, il existerait r , $1 \leq r \leq a_2$ tel que $\|(rq_1+1)\frac{a}{p} - h\frac{a}{p}\| < \|q_1\frac{a}{p}\|$, ce qui est impossible si $h < q_2$. D'où $\underbrace{h\frac{a}{p}} \geq \frac{a}{p} + \frac{1}{p} = \underbrace{(q_2+1)\frac{a}{p}}$; l'égalité est impossible car $h < q_2$ on a donc dans ce cas : $\underbrace{h\frac{a}{p}} > \frac{a}{p} + \underbrace{(J+1)\frac{a}{p}}$. On en déduit :

$$\mu_{j,i}^{-(J)} \neq 0 \quad \text{pour } m \leq j \leq m+d_m$$

d'autre part :

$$\mu_{j,i}^{-(J)} = 0 \quad \text{si } j < m \quad \text{ou } j > m+d_m .$$

Donnons un exemple pour écrire dans un cas particulier la matrice $M(\frac{f^J}{v_J})$.

Soit K/k une extension où : $p = 7$, $t = a = 4$ et $e_0 = 4$. (Il en existe d'après le rappel du §1.3 de ce chapitre). n est égal à 3 , en effet $\frac{4}{7} = \frac{1}{1+\frac{1}{1+\frac{1}{3}}} = [0,1,1,3]$; c'est-à-dire : $a_1 = 1$, $a_2 = 1$, $a_3 = 3$, $q_1 = 1$, $q_2 = 2$, $q_3 = 7$.

Rassemblons les suites v_i et n_i , $0 \leq i \leq 6$ dans un tableau :

i	1	2	3	4	5	6
$v_i = [\frac{it+a}{p}]$	1	1	2	2	3	4
n_i	0	1	1	2	3	4

$J = q_2 - 1 = 1$, écrivons $M(\frac{f^J}{v_J})$ modulo $\overline{w}$, c'est-à-dire $\overline{M(\frac{f}{w})}$:

$$\overline{M(\frac{f}{w})} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & a \\ 0 & 1 & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{où } a \text{ et } b \text{ sont deux éléments non nuls de } \overline{k} .$$

Cas $n = 4$. $E = \{1, q_1+1, 2q_1+1, \dots, q_2, q_3+q_2, 2q_3+q_2, \dots, (a_4-1)q_3+q_2\}$.

Etudions encore la matrice $M(\frac{f^J}{v_J})$ en nous servant du lemme 5 .

Décrivons la i -ème colonne de cette matrice, $0 \leq i \leq p-1$, et posons $h = p-i$.

■ Si $h \geq J+1 = q_2$: $\overline{\mu}_{J+i,i}^{(J)} = 1$ et $\overline{\mu}_{j,i}^{(J)} = 0$ pour j différent de $J+i$.

En effet, comme $\|q_3 \frac{a}{p}\| = \frac{1}{p}$, les seuls entiers k vérifiant :

$\underbrace{k \frac{a}{p}} < \underbrace{q_2 \frac{a}{p}}$ sont les entiers : q_2+q_3 , $2q_3+q_2$, $\dots$, $(a_4-1)q_3 + q_2$ de E .

Donc, si h n'appartient pas à E on a : $\underbrace{(J+1) \frac{a}{p}} < \underbrace{h \frac{a}{p}}$.

■ Si $h < J+1$ c'est-à-dire $h \leq q_2-1$ posons $i+J = p-1+m$,

- Supposons h dans E . h étant inférieur à q_2 on a

$$\underbrace{h \frac{a}{p}} > \underbrace{(J+1) \frac{a}{p}} = \underbrace{q_2 \frac{a}{p}} \quad \text{et} \quad 1 + \underbrace{h \frac{a}{p}} > \frac{a}{p} + \underbrace{(J+1) \frac{a}{p}} \quad \text{on en déduit :}$$

$$\bar{\mu}_{j,i}^{(J)} \neq 0 \quad \text{pour} \quad m \leq j \leq m+d_m.$$

D'autre part :

$$\bar{\mu}_{j,i}^{(J)} = 0 \quad \text{pour} \quad j < m \quad \text{ou} \quad j > m+d_m.$$

- Supposons h hors de E . On a $\underbrace{h \frac{a}{p}} > \frac{a}{p} + \underbrace{q_2 \frac{a}{p}}$, en effet $\underbrace{h \frac{a}{p}} > \frac{a}{p}$ (même raisonnement que ci-dessus). Or l'inégalité : $\underbrace{h \frac{a}{p}} - \frac{a}{p} \leq \underbrace{q_2 \frac{a}{p}}$, signifierait que $\|h \frac{a}{p} - \frac{a}{p}\| \leq \|q_2 \frac{a}{p}\|$, ce qui est impossible pour $h < q_2$.

La matrice $M(\frac{f}{\bar{v}_J})$ est du même type dans le cas $n = 4$ que dans le cas $n = 3$.

Ecrivons la matrice $M(\alpha)$ dans ces deux cas. Elle s'obtient en mettant sur la diagonale de la matrice précédente des u sur les lignes d'indice i , tel que $n_i = v_i$ et des $\bar{u}$ sur les autres.

Si nous l'écrivons dans le cas de l'exemple précédent on obtient :

$$\text{si } \alpha = u + \frac{f}{\bar{w}}$$

$$\overline{M(\alpha)} = \begin{pmatrix} \bar{u} & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & a \\ 0 & 1 & \bar{u} & 0 & 0 & 0 & b \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \bar{u} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \bar{u} & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & \bar{u} \end{pmatrix}.$$

Calculons le déterminant de $\overline{M(\alpha)}$, ce qui donnera le déterminant de $M(\alpha)$ modulo $\bar{w}$. En développant ce déterminant par rapport à la première ligne il s'écrit : $\det \overline{M(\alpha)} = \bar{u} \det M'$, où M' est la matrice d'ordre $p-1$ obtenue en supprimant la première ligne et la première colonne de $\overline{M(\alpha)}$. Le déterminant de M' n'a qu'un seul terme indépendant de $\bar{u}$ c'est le terme

$$b_o = \prod_{i=0}^{p-1} \bar{\mu}_{j+i,i}^{(J)} \times \prod_{i=p-1-J}^{p-1} \bar{\mu}_{m_i,i}^{(J)} \quad \text{où} \quad m_i = i+J-p+1;$$

b_o est une unité ; les autres termes ont en facteur une puissance de $\bar{u}$ inférieure ou égale à $p-2$, car si a ne divise pas $p-1$, $\bar{u}_0$ est différent de

$\mathfrak{D}$ et par suite on a au moins un élément nul sur la diagonale. Il existe donc un polynôme P de $A[X]$ de degré inférieur ou égal à $p-2$, ne dépendant pas de u , tel que le déterminant de $M(\alpha)$ soit congru à $uP(u)$ modulo $\overline{w}A$, avec $\overline{P(0)} \neq 0$. P étant de degré $p-2$, $\overline{P}$ n'est pas identiquement nul dans $\overline{K}$ et il existe des unités u dans A telles que le déterminant de $M(\alpha)$ ne soit pas congru à zéro modulo $\overline{w}A$, ce qui achève la démonstration de la proposition 6.

Proposition 7.

Si l'entier n est supérieur ou égal à 5, $\mathfrak{u}_\theta$ n'est pas un idéal principal de l'ordre $\mathfrak{D}$.

Démonstration de la proposition 7 :

Notons $\alpha = \sum_{J=0}^{p-1} x_J \frac{f^J}{\overline{w}^J}$, un élément quelconque de l'idéal $\mathfrak{u}_\theta$ et posons :
 $n = 2s+1$ si n est impair et $n = 2s+2$ si n est pair.

Considérons les colonnes de la matrice $M(\alpha)$ d'indice i , où $h = p-1$ prend les valeurs : $h = 2q_{2s-2}$, $h = q_{2s-2} + a'_{2s}q_{2s-1} + q_{2s}$ avec $0 \leq a'_{2s} \leq a_{2s}$; ces valeurs de h n'appartiennent pas à E ; le lemme 5 permet de montrer les résultats suivants :

a) si $J+1 \leq h$, les valeurs de J pour lesquelles : $\overline{\mu}_{J+1,1}^{(J)} \neq 0$,
sont données par : $J+1 = q_{2s-2}$ pour $h = 2q_{2s-2}$ et $J+1 = q_{2s-2} + a''_{2s}q_{2s-1}$
pour $h = q_{2s-2} + a'_{2s}q_{2s-1} + q_{2s}$ avec $a'_{2s} \leq a''_{2s} \leq a_{2s}$.

D'après le lemme 5 les valeurs de J sont celles pour lesquelles :

$$\underbrace{(J+1)}_{< h} \frac{a}{p} < \underbrace{h}_{> J+1} \frac{a}{p}.$$

Fixons $\lambda = a'_{2s}q_{2s-1} + q_{2s-2}$, $0 \leq a'_{2s} \leq a_{2s}$ et $h = q_{2s} + \lambda$.

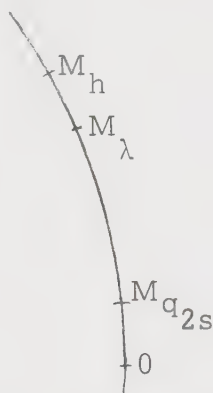
Montrons que si $J+1 < h$ et si $\underbrace{(J+1)}_{< h} \frac{a}{p} < \underbrace{h}_{> J+1} \frac{a}{p}$ alors $J+1$ est dans E et de plus $\lambda \leq J+1 \leq q_{2s}$.

■ $J+1 < h \leq 2q_{2s}$, donc $J+1 - q_{2s} < \lambda$ et comme λ est dans E on a :

$$\underbrace{(1 + 1 - q_{2s})}_{< \lambda} \frac{a}{p} > \underbrace{\lambda}_{> J+1} \frac{a}{p}.$$

■ Si $\underbrace{(J+1)\frac{a}{p}} < \underbrace{h\frac{a}{p}}$, le point M_{J+1} du cercle (C) (cf. démonstration du lemme 4) est entre le point 0 et le point M_h .

Disposons sur le cercle (C) les points $M_{q_{2s}}$, M_h et M_λ .



■ Si le point M_{J+1} est entre les points 0 et $M_{q_{2s}}$, on a $n = 2s + 2$ et $J+1 = xq_{2s+1} + q_{2s}$ avec $0 \leq x \leq a_{2s+2}$, mais alors $J+1$ est strictement supérieur à $2q_{2s}$, ce qui est impossible.

■ Si le point M_{J+1} est entre $M_{q_{2s}}$ et M_h et que de plus : $J+1 > q_{2s}$ alors $\underbrace{(J+1-q_{2s})\frac{a}{p}} < \underbrace{\lambda\frac{a}{p}}$, ce qui est impossible.

Donc $J+1 \leq 2q_{2s}$.

■ $\underbrace{(J+1)\frac{a}{p}} < \underbrace{h\frac{a}{p}} = \underbrace{q_{2s}\frac{a}{p}} + \underbrace{\lambda\frac{a}{p}}$ entraîne que : $\underbrace{(J+1)\frac{a}{p}} \leq \underbrace{\lambda\frac{a}{p}}$.

En effet, on ne peut avoir $\underbrace{(J+1)\frac{a}{p}} > \underbrace{\lambda\frac{a}{p}}$ car $J+1$ et λ étant tous deux inférieurs à q_{2s} on a : $\|(J+1-\lambda)\frac{a}{p}\| > \delta_{2s} = \underbrace{q_{2s}\frac{a}{p}}$ (cf. démonstration du lemme 4). λ appartenant à E , si $\underbrace{(J+1)\frac{a}{p}} \leq \underbrace{\lambda\frac{a}{p}}$ c'est que : $\lambda \leq J+1$.

On a montré que : $\lambda \leq J+1 \leq q_{2s}$.

Les valeurs de J qui conviennent sont celles qui correspondent à des points M_{J+1} se trouvant entre $M_{q_{2s}}$ et M_h . Or si $|i-j| < q_{2s}$, $\|(i-j)\frac{a}{p}\| \geq \delta_{2s-1}$. Les seules valeurs possibles sont donc :

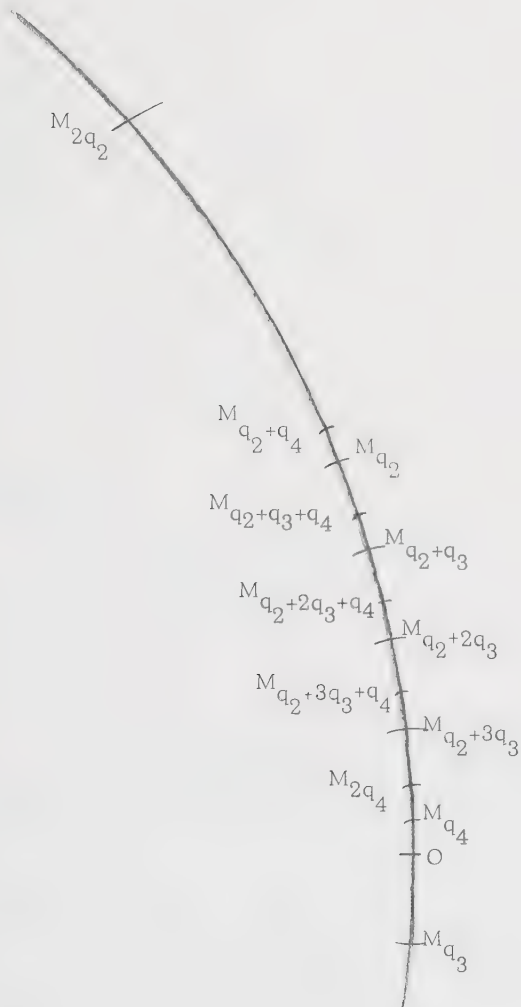
$$J+1 = a''_{2s}q_{2s-1} + q_{2s-2} \quad \text{où} \quad a'_{2s} \leq a''_{2s} \leq a_{2s}.$$

b) Si $J+1 < h$, quel que soit j : $\bar{\mu}_{j,i}^{(J)} = 0$.

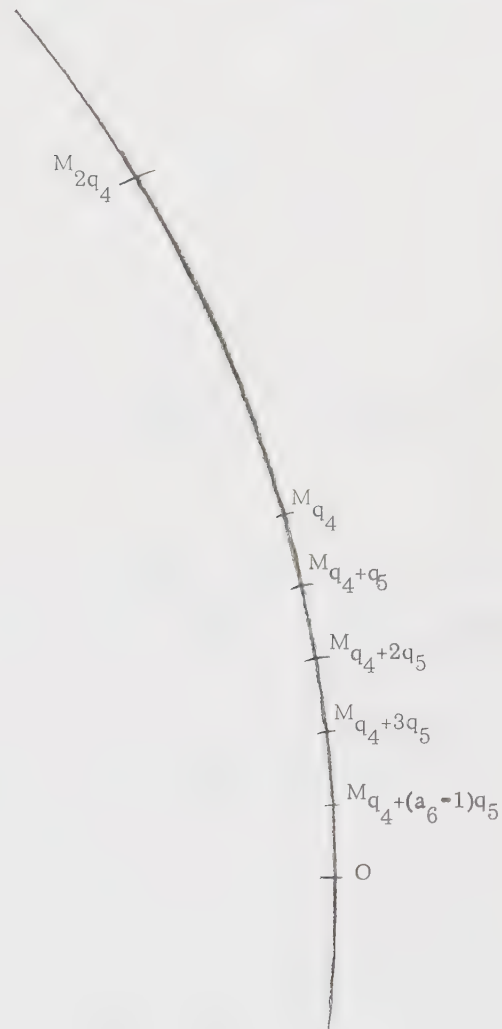
En effet, pour tous les h choisis ; $\underbrace{h \frac{a}{p}} < \frac{a}{p}$.

Illustrons ces résultats dans les cas $n = 5$ et $n = 6$:

$n = 5$



$n = 6$



En résumé, sur les colonnes d'indices i ci-dessus de la matrice $M(\alpha)$, colonnes qui sont au nombre de a_{2s+2} , les seuls éléments susceptibles d'être non nuls modulo $\overline{w}A$ sont sur les a_{2s+1} lignes d'indice j donnés par :

$$p-j-1 = q_{2s-2} + a'_{2s} q_{2s-1} \quad \text{avec} \quad 0 \leq a'_{2s} \leq a_{2s}.$$

Il en résulte que le déterminant de $M(\alpha)$ est congru à zéro modulo $\overline{w}A$ pour tout α de $\mathfrak{U}_\theta$.

Donnons un exemple illustrant la proposition 7.

Soit $p = 13$, $t = a = 8$, $e_o = 8$, on a $\frac{8}{13} = [0,1,1,1,1,2]$
c'est-à-dire $a_1 = 1$, $a_2 = 1$, $a_3 = 1$, $a_4 = 1$, $a_5 = 2$ et $q_1 = 1$,
 $q_2 = 2$, $q_3 = 3$, $q_4 = 5$, $q_5 = 13$.

$n = 5$ et par suite $s = 2$. Considérons les colonnes de $M(\alpha)$
d'indice i où $h = p-i$ prend les valeurs $h = 2q_2 = 4$, $h = q_2 + q_4 = 7$,
 $h = q_2 + q_3 + q_4 = 10$. C'est-à-dire $i = 3$, $i = 6$, $i = 9$. Sur ces trois
colonnes les seuls coefficients de $M(\alpha)$ non congrus à zéro modulo $\overline{w}$ se
trouvent sur les lignes $j = 7$ et $j = 10$ d'après la démonstration de la
proposition 7. On peut le vérifier directement en utilisant les suites n_i et
 v_i , $0 \leq i \leq p-1$.

5.2.3. On peut résumer les résultats obtenus dans le théorème :

Théorème 2.

Si l'indice de ramification t , est "presque maximal" , pour que B
soit un $\mathfrak{D}$ -module libre, il faut et il suffit que l'entier n soit inférieur ou
égal à 4 .

De ce théorème 2 on peut déduire le corollaire 3, comme on a déduit
du théorème 1 de ce chapitre le corollaire 1.

Corollaire 3.

Pour que B soit un $\mathfrak{D}$ -module projectif, si t est presque maximal,
il faut et il suffit que l'entier n soit inférieur ou égal à 4 .

Exemples :

Si $p = 7$, $t = 5$, $e_o = 5$, t vérifie (I) et $n = 3$, B est libre sur $\mathfrak{D}$.

Si $p = 11$, $t = 4$, $e_o = 4$, t vérifie (I) et $n = 3$, B est libre sur $\mathfrak{D}$.

Si $p = 13$, $t = 8$, $e_o = 8$, t vérifie (I) et $n = 5$, B n'est pas projectif sur $\mathfrak{D}$.

(On sait qu'il existe des extensions K/k , avec p , t , e_o , comme ci-
dessus (chapitre II, §1.3).

5.2.4. Le problème posé au début de ce chapitre est donc résolu ; on a caractérisé toutes les extensions cycliques de degré p , K/k , d'un corps local pour lesquelles B est libre sur son ordre associé dans $k[G]$.

Résumons les résultats obtenus :

- a) si $t < \frac{pe_o}{p-1} - 1$; B est libre sur $\mathfrak{O}$ si et seulement si a divise $p-1$.
- b) si $\frac{pe_o}{p-1} - 1 \leq t \leq \frac{pe_o}{p-1}$; B est libre sur $\mathfrak{O}$ si et seulement si, dans le développement en fraction continue $\frac{t}{p} = [a_o, a_1, \dots, a_n]$ où $a_n > 1$, n est inférieur ou égal à 4.

Dans la fin de ce chapitre, nous chercherons dans quels cas l'égalité : $\mathfrak{O} = \mathfrak{O}_m$ est vérifiée, t satisfaisant toujours à l'inégalité (I).

5.3. Comparaison de $\mathfrak{O}$ et $\mathfrak{O}_m$.

5.3.1. On se propose de comparer l'ordre $\mathfrak{O}$ associé à B dans l'algèbre $k[G]$ et l'ordre maximal $\mathfrak{O}_m$, de $k[G]$; on montre que $\mathfrak{O}_m$ est donné par :

Lemme 6.

L'ordre maximal, $\mathfrak{O}_m$, de $k[G]$ est le sous A -module de $k[G]$ engendré par la famille $\left(\frac{f^i}{[\frac{ie_o}{p-1}]} \right)_{0 \leq i \leq p-1}$.

Démonstration :

- a) Montrons que pour $0 \leq i \leq p-1$, $\frac{f^i}{[\frac{ie_o}{p-1}]}$ est un élément de $\mathfrak{O}_m$.

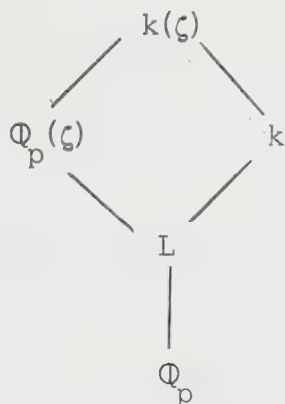
Si le polynôme X^{p-1} se décompose sur k de la façon suivante :

$$X^{p-1} = (X-1) \cdot P_1(X) \cdot P_2(X) \dots P_r(X)$$

où les P_i sont des polynômes irréductibles à coefficients dans k , de même degré n puisqu'ils engendrent tous l'extension $k(\zeta)/k$, (ζ racine primitive p -ème de l'unité), alors on a l'isomorphisme :

$$k[G] \simeq k \times \underbrace{k(\zeta) \times k(\zeta) \times \dots \times k(\zeta)}_{r \text{ fois}},$$

et le schéma suivant :



où $L = \mathbb{Q}_p(\zeta) \cap k$, $r = [L:\mathbb{Q}_p]$, $n = [\mathbb{Q}_p(\zeta):L] = [k(\zeta):k]$ et $p-1 = nr$.

Posons $e_0 = re_1$, $e_1 = de'$ et $n = dq$ où d est le plus grand diviseur commun à n et e_1 . q est l'indice de ramification de l'extension $k(\zeta)/k$. En effet, on voit facilement que cet indice est multiple de q , puis on montre que l'extension $k\{(1-\zeta)^q\}/k$ est non ramifiée, car $\frac{(1-\zeta)^q}{w^{e'}}$ est une unité qui engendre l'extension résiduelle.

Dans l'extension $k(\zeta)/k$, $\frac{(1-\zeta)^i}{w^\lambda}$ est donc un entier si et seulement si $ie' - q\lambda \geq 0$, c'est-à-dire si et seulement si :

$$\lambda \leq \frac{ie'}{q} = \frac{ie_0}{p-1}.$$

L'isomorphisme vu plus haut montre que $\mathfrak{O}_m$ est isomorphe au produit direct :

$$\mathfrak{O}_m \simeq A \times \underbrace{A_1 \times A_1 \times \dots \times A_1}_{r \text{ fois}} \quad \text{où } A_1 \text{ est l'anneau des entiers de } k(\zeta).$$

Par suite, $\frac{f^i}{\left[\frac{ie_0}{p-1}\right] w}$, pour $0 \leq i \leq p-1$, est un élément de $\mathfrak{O}_m$.

b) Soit $\mathfrak{O}'$, l'ordre de $k[G]$ engendré par la famille : $\left(\frac{f^i}{\left[\frac{ie_0}{p-1}\right] w} \right)_{0 \leq i \leq p-1}$.

Montrons que $\mathfrak{O}'$ est l'ordre maximal $\mathfrak{O}_m$ de $k[G]$. Pour cela, il suffit de vérifier que le discriminant de $\mathfrak{O}'$, $\Delta(\mathfrak{O}')$, est égal au discriminant, Δ , de l'algèbre $k[G]$. [3].

Grâce à l'isomorphisme vu ci-dessus, le calcul de Δ se ramène au calcul du discriminant de $k(\zeta)/k$ que nous notons δ .

En effet : $\Delta = \delta^r$.

Calculons δ . L'extension $k(\zeta)/k$ étant modérément ramifiée, d'indice de ramification q , on a : $\delta = \varpi^{d(q-1)}$ et par suite :

$$\Delta = \varpi^{rd(q-1)}.$$

Calculons à présent le discriminant $\Delta(\mathfrak{D}')$. Dans $k[G]$ le discriminant de la base $(1, f, \dots, f^{p-1})$ est : $\Delta(1, f, \dots, f^{p-1}) = p^p$. Par suite :

$$\Delta(\mathfrak{D}') = \begin{vmatrix} 1 & 0 & \dots & \dots & \dots & 0 \\ & \varpi^{-\frac{e_0}{p-1}} & & & & \\ 0 & \varpi & & & & \\ & & \varpi^{2e_0} & & & \\ \vdots & 0 & \varpi & & & \\ & & & 0 & & \\ \vdots & & & & \ddots & \\ & & & & & 0 \\ \vdots & & & & & \\ & & & & & 0 \\ 0 & \dots & \dots & \dots & \dots & \varpi^{-e_0} \end{vmatrix}^2 \quad \Delta(1, f, \dots, f^{p-1}) = m^2 p^p.$$

$$\text{Et } m^2 = \varpi^{-2 \sum_{i=0}^{p-1} \left[\frac{ie_0}{p-1} \right]}.$$

Calculons de manière générale : $\sum_{i=0}^{c-1} \left[i \frac{b}{c} \right]$ où b et c sont deux entiers positifs premiers entre eux.

$$\sum_{i=0}^{c-1} \left[i \frac{b}{c} \right] + \sum_{i=0}^{c-1} i \frac{b}{c} = \frac{b}{c} \times \frac{1}{2} c(c-1) = \frac{b(c-1)}{2}$$

$$\sum_{i=0}^{c-1} i \frac{b}{c} = \frac{1}{c} + \frac{2}{c} + \dots + \frac{c-1}{c} = \frac{c-1}{2}$$

On a donc :

$$\sum_{i=0}^{c-1} \left[i \frac{b}{c} \right] = \frac{(b-1)(c-1)}{2}. \quad (3)$$

Dans notre cas $\sum_{i=0}^{p-1} \frac{ie_0}{p-1} = \sum_{i=0}^{p-1} i \frac{e'}{q} = rd \sum_{i=0}^{q-1} i \frac{e'}{q} = rd \frac{(q-1)}{2}$

et

$$\sum_{i=0}^{p-1} \left[\frac{ie_0}{p-1} \right] = \sum_{i=0}^{p-1} i \frac{e_0}{p-1} - rd \frac{(q-1)}{2}.$$

Nous avons donc
$$\sum_{i=0}^{p-1} \left[\frac{ie_0}{p-1} \right] = \frac{1}{2}(pe_0 - rd(q-1)) .$$

$$\text{Par suite } \Delta(\mathfrak{D}') = \frac{p^p}{pe_0 - rd(q-1)} = w^{rd(q-1)}$$

on a bien $\Delta(\mathfrak{D}') = \Delta$

et par suite $\mathfrak{D}' = \mathfrak{D}_m .$

5.3.2. On sait que pour toute extension K/k on a l'inclusion : $\mathfrak{D} \subset \mathfrak{D}_m$. Une condition nécessaire et suffisante pour que $\mathfrak{D} = \mathfrak{D}_m$ est que le discriminant de l'ordre associé, $\mathfrak{D}$, soit égal à $\Delta = \Delta(\mathfrak{D}_m)$.

Lemme 7.

On suppose que t vérifie (I) . Pour que $\mathfrak{D} = \mathfrak{D}_m$ il faut et il suffit que :

$$2 \text{ Card } E = a + (a, p-1)$$

où Card E désigne le cardinal de l'ensemble E défini dans ce paragraphe et où $(a, p-1)$ désigne le plus grand diviseur commun à a et $p-1$.

Démonstration :

$\mathfrak{D} = \mathfrak{D}_m$ si et seulement si $\Delta(\mathfrak{D}) = \Delta(\mathfrak{D}_m)$.

Calculons $\Delta(\mathfrak{D})$. $\mathfrak{D}$ est le sous A -module de $k[G]$ engendré par la famille $\left(\frac{f^i}{n_i} \right)_{0 \leq i \leq p-1}$ où n_i est donné par (proposition 5 du chapitre II) :

$$n_i = ia_0 + \left[i \frac{a}{p} \right] + \begin{cases} 0 & \text{si } p-i \text{ n'appartient pas à } E \\ 1 & \text{si } p-i \text{ appartient à } E . \end{cases}$$

Comme précédemment, $\Delta(\mathfrak{D}) = m'^2 \Delta(1, f, \dots, f^{p-1})$ où $m'^2 = w^{-2 \sum_{i=0}^{p-1} n_i}$.

Par suite $\mathfrak{D} = \mathfrak{D}_m$ si et seulement si ; $\sum_{i=0}^{p-1} n_i = \sum_{i=0}^{p-1} \left[\frac{ie_0}{p-1} \right] .$

D'après la formule (3) :

$$\sum_{i=0}^{p-1} n_i = \sum_{i=0}^{p-1} ia_0 + \sum_{i=0}^{p-1} \left[i \frac{a}{p} \right] + \text{Card } E = a_0 \frac{p(p-1)}{2} + \frac{(a-1)(p-1)}{2} + \text{Card } E$$

$$\sum_{i=0}^{p-1} n_i = \frac{pe_0}{2} - \frac{p-1}{2} - \frac{a}{2} + \text{Card } E$$

$$\sum_{i=0}^{p-1} \left[\frac{ie_0}{p-1} \right] = \frac{pe_0}{2} - \frac{p-1}{2} + \frac{rd}{2} = \frac{pe_0}{2} - \frac{p-1}{2} + \frac{(a, p-1)}{2} .$$

On a donc $\mathfrak{D} = \mathfrak{D}_m$ si et seulement si : $2 \text{ Card } E = a + (a, p-1)$.

Théorème 3.

Pour que l'ordre $\mathfrak{D}$, associé à B , coïncide avec $\mathfrak{D}_m$, ordre maximal de $k[G]$, il faut et il suffit que le nombre de ramification de l'extension, t , vérifie la double inégalité (I) et que a , reste de t modulo p , vérifie l'une des quatre conditions suivantes :

a est nul , ou a divise p-1 , ou a divise p-2 , ou a divise 2p-1 .

Démonstration du théorème 3 :

On sait que $\mathfrak{D}_m$ est un anneau dont tout idéal est principal. La proposition 7 de ce chapitre montre donc que si $n \geq 5$, $\mathfrak{D}$ est différent de $\mathfrak{D}_m$. Il nous reste à étudier les cas $n \leq 4$.

Cas $n = 0$: $a = 0$, on sait que t vérifie (I) et que $\mathfrak{D} = \mathfrak{D}_m$ (chapitre II, prop.1).

Cas $n = 1$: $a = 1$.

Cas $n = 2$: $a \neq 1$ et a divise p-1 ; dans ces deux cas pour que $\mathfrak{D} = \mathfrak{D}_m$ il est nécessaire que t vérifie (I) (cf. remarque du §3 du chapitre II). On vérifie directement que cette condition est suffisante, en effet on a :

$$n_i = v_i = ia_0 + [(i+1)\frac{a}{p}] \quad (\text{Prop.2, chapitre II})$$

et si t vérifie (I) $e_0 = (p-1)a_0 + a$ d'où $n_1 = \left[\frac{ie_0}{p-1} \right]$.

Cas $n = 3$: Il y a dans ce cas a_2+1 éléments dans E et comme :

$$\frac{p}{a} = a_1 + \frac{1}{a_2 + \frac{1}{a_3}} , \quad a = a_2 a_3 + 1 .$$

Par suite $\mathfrak{D} = \mathfrak{D}_m$ si et seulement si : $2a_2+2 = a_2 a_3 + 1 + (a, p-1)$.

Si $(a, p-1)$ était strictement supérieur à 1 , a_3 serait strictement inférieur

à 2 ce qui est impossible lorsque $n = 3$ car $a_3 > 1$. On a donc :
 $(a, p-1) = 1$ et $a_3 = 2$.

Dans le cas $n = 3$, $\mathfrak{D}$ est égal à $\mathfrak{D}_m$ si et seulement si $a_3 = 2$,
ce qui équivaut à : a divise $p-2$.

Cas $n = 4$: Card $E = a_4 + 1$ et comme : $\frac{p}{a} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4}}}$,

$$a = a_2 + a_4 + a_2 a_3 a_4.$$

Par suite $\mathfrak{D} = \mathfrak{D}_m$ si et seulement si : $2a_4 + 2 = a_2 + a_4 + a_2 a_3 a_4 + (a, p-1)$.
 On voit que $(a, p-1)$ doit encore être égal à 1 et que $a_2 = a_3 = 1$.

Dans le cas $n = 4$, $\mathfrak{D}$ est donc égal à $\mathfrak{D}_m$ si et seulement si
 $a_2 = a_3 = 1$, ce qui équivaut à a divise $2p-1$.

Ceci termine la démonstration du théorème 3.

Exemples.

$$p = 7, t = 5, e_o = 5; \frac{t}{p} = [0, 1, 2, 2] \text{ et } \mathfrak{D} = \mathfrak{D}_m$$

$$p = 11, t = 4, e_o = 4; \frac{t}{p} = [0, 2, 1, 3] \text{ et } \mathfrak{D} \neq \mathfrak{D}_m$$

$$p = 13, t = 8, e_o = 8; \frac{t}{p} = [0, 1, 1, 1, 1, 2] \text{ et } \mathfrak{D} \neq \mathfrak{D}_m.$$

CHAPITRE III

CAS D'UNE EXTENSION DIEDRALE DE DEGRE $2p$ D'UN CORPS LOCAL

1. NOTATIONS.

Dans le chapitre III, F désigne un corps local de caractéristique zéro et de caractéristique résiduelle p , p nombre premier impair. G est un groupe diédral d'ordre $2p$ et K une extension galoisienne de F avec $G = \text{Gal}(K/F)$.

On note :

- A l'anneau des entiers de F , e_o l'indice de ramification absolu de F ;
- σ et τ les deux générateurs de G tels que : $\sigma^p = \tau^2 = 1$ et $\sigma\tau = \tau\sigma^{-1}$;
- H le sous-groupe de G engendré par σ , g l'élément de $F[G]$ défini par : $g = \sigma - \sigma^{-1}$;
- k le sous-corps de K correspondant au groupe H , B et C les anneaux d'entiers respectifs de k et de K ;
- v_K la valuation normalisée de K ;
- π , ϖ' et ϖ des uniformisantes respectives de K , k et F ;
- $(u, \tau.u)$ une base du A -module B ; (base normale de l'extension k/F modérément ramifiée).
- t , l'entier défini par $G_t \neq \{1\}$ et $G_t = \{1\}$; (G_i , pour i entier positif ou nul, désigne le i -ème groupe de ramification de G) .

Posons $t = a_o p + a$, a étant le plus petit entier positif ou nul congru à t modulo p .

Si x est un nombre réel, on note $[x]$ sa partie entière et $\underline{x}$ sa partie fractionnaire de sorte que : $x = [x] + \underline{x}$ avec $0 \leq \underline{x} < 1$.

$\mathfrak{D}$ est dans ce chapitre l'ordre associé à C dans $F[G]$, c'est-à-dire :

$$\mathfrak{D} = \{\lambda \in F[G] ; \lambda C \subset C\}.$$

Si θ est un élément de C engendrant une base normale de K/F , on note $\mathfrak{U}_\theta$ le sous $A[G]$ -module de $F[G]$ défini par :

$$\mathfrak{U}_\theta = \{\lambda \in F[G] ; \lambda \theta \in C\}.$$

2. REMARQUES.

2.1. Si K/F est une extension diédrale modérément ramifiée, on sait que C est libre sur $A[G]$; [8] ; dans ce cas $A[G] = \mathfrak{D}$.

Dans la suite, on ne considèrera donc que des extensions sauvagement ramifiées, ($t \geq 1$). On distinguera deux cas suivant que k/F est ramifiée ou non, cas désignés respectivement par A et B .

La numération des propositions qui correspondent seulement au cas A (respectivement B) sera suivie d'un (A), (resp (B)).

2.2. Dans le cas A (l'extension K/F est totalement ramifiée), on a :

$$1 \leq t \leq \frac{2pe_o}{p-1} \quad ([12] \text{ ch.IV } \S 2 \text{ exercice 3})$$

et t est impair d'après [8]. a_o et a sont donc dans ce cas de parité différente.

Dans le cas B (l'extension K/F n'est ramifiée que dans la partie K/k) on a :

$$1 \leq t \leq \frac{pe_o}{p-1} \quad ([12]).$$

2.3. Montrons qu'on peut choisir une uniformisante π de K vérifiant les conditions suivantes :

dans le cas A : $\tau\pi = -\pi$ et si $a = 0$, π^p appartient à k ;

dans le cas B : $\tau\pi = \pi$ et si $a = 0$, π^p appartient à F .

- Cas A avec $a \neq 0$. L'extension K/F étant totalement ramifiée on a quelle que soit une uniformisante π' de K : $\tau\pi' - \pi' = \epsilon\pi'$ où ϵ est une unité de K .

Si l'on pose $\pi = \epsilon\pi'$, π est une uniformisante de K telle que :

$$\tau\pi = -\pi .$$

- Cas A avec $a = 0$. D'après le paragraphe 1.3.c) du chapitre II, k contient les racines p -èmes de l'unité et il existe une uniformisante π' de K telle que π'^p soit une uniformisante de k avec $\sigma.\pi' = \zeta\pi'$, ζ racine primitive p -ème de l'unité. On montre que $\tau.\zeta = \zeta^{-1}$. En effet, si $\tau.\zeta = \zeta^i$, comme $\tau^2.\zeta = \zeta$, i doit être égal à 1 ou à -1 ; or si $p \neq 2$ et $\tau.\zeta = \zeta$, on montre que $\sigma\tau.\pi' \neq \tau\sigma^{p-1}.\pi'$ ce qui est impossible. Par suite $\tau.\zeta = \zeta^{-1}$ et F ne contient pas ζ . On déduit, de ce qui précède qu'il existe un entier i $0 \leq i \leq p-1$ tel que $\tau(\zeta^i\pi') = -(\zeta^i\pi')$. En posant $\pi = \zeta^i\pi'$ on a : $\tau\pi = -\pi$ et π^p uniformisante de k .

- Cas B avec $a \neq 0$. L'extension k/F étant non ramifiée, on peut choisir π telle que $\tau\pi = \pi$; il suffit pour cela de prendre pour π une uniformisante de k' , si k' est le sous-corps de K , galoisien sur F et tel que $[k':F] = p$.

- Cas B avec $a = 0$. Comme dans le cas A , k contient les racines p -èmes de l'unité et il existe une uniformisante π' de K telle que π'^p soit uniformisante de k et que $\sigma.\pi' = \zeta\pi'$. Alors on montre de façon analogue que : $\tau.\zeta = \zeta^{-1}$ et qu'il existe un entier i , $0 \leq i \leq p-1$ tel que : $\tau.(\zeta^i\pi') = \zeta^i\pi'$. En posant $\pi = \zeta^i\pi'$ on voit que $\tau\pi = \pi$ et que π^p est une uniformisante de F .

Dans toute la suite π sera dans chacun des cas une uniformisante vérifiant ces conditions.

2.4. On montre à l'aide de la théorie de Kummer [11] qu'il existe des extensions de corps locaux, K/F , diédrales de degré $2p$ (cas A et cas B) pour

lesquelles l'entier a prend une valeur quelconque de zéro à $p-1$.

D'après Hasse [4 bis] si k/F est une extension cyclique (groupe de Galois engendré par τ), si k contient les racines n -èmes de l'unité et si $K = k(\alpha^{1/n})$ est une extension cyclique de degré n de k (α élément de k) alors :

1) K/F est une extension galoisienne si et seulement si, il existe j dans $\mathbb{Z}$, $j \neq 0$, et λ dans k tels que : $\tau \cdot \alpha = \alpha^j \lambda^n$.

2) K/F est abélienne si et seulement si $\tau \cdot \alpha = \alpha^i \lambda^n$ où λ est dans k et où i est défini modulo n par $\tau \cdot \zeta = \zeta^i$ (ζ racine n -ème de l'unité).

On remarque qu'une extension galoisienne non abélienne de degré $2p$ est une extension diédrale.

Soit $K = k(\alpha^{1/p})$ une extension de Kummer du corps k , où p est un nombre premier, on désigne par e'_0 l'indice de ramification absolu de k et par $\overline{w}$ une uniformisante de k .

Supposons : $\alpha = 1 + \lambda \overline{w}^u$, où u est un entier supérieur ou égal à 1 et où λ est une unité de k ; les résultats de [11] peuvent alors s'énoncer sous la forme suivante :

1) si $u \geq \frac{pe'_0}{p-1} + 1$, α est une puissance p -ème dans k .

si $u < \frac{pe'_0}{p-1}$ et si u est premier à p , α n'est pas une puissance p -ème de k .

2) Supposons : $u < \frac{pe'_0}{p-1}$ et u premier à p ; le nombre de ramification, t , de l'extension cyclique K/k est donné par :

$$t = \frac{pe'_0}{p-1} - u.$$

Pour donner des exemples où t prend toutes les valeurs possibles, on utilisera le lemme suivant :

Lemme.

Soit k/F une extension quadratique de corps locaux ; on suppose que k contient les racines p -èmes de l'unité et que F ne les contient pas. Soit t , un entier vérifiant l'une des deux conditions suivantes (e'_0 indice de ramification absolu de k) :

$$a) \quad t = \frac{pe'_0}{p-1} ;$$

$$b) \quad 1 \leq t < \frac{pe'_0}{p-1}, \quad t \text{ premier à } p \text{ et si } k/F \text{ est ramifiée } t \text{ impair.}$$

Il existe une extension K de k , telle que l'extension K/F soit diédrale et ait pour nombre de ramification t .

Démonstration :

Choisissons une uniformisante ϖ' de k telle que :

$$\tau \cdot \varpi' = -\varpi' \quad \text{si } k/F \text{ est ramifiée}$$

$$\tau \cdot \varpi' = \varpi' \quad \text{si } k/F \text{ n'est pas ramifiée.}$$

Ce choix est possible d'après le §2.3 précédent.

a) Prenons $\alpha = \varpi'$ et $K = k(\varpi'^{1/p})$. On a $\tau\alpha = \pm\alpha$, K/F est donc une extension de Galois, de plus comme $\tau\zeta = \zeta^{-1}$ (F ne contient pas ζ), K/F est une extension diédrale.

Dans cette situation on a vu que $t = \frac{pe'_0}{p-1}$ était le nombre de ramification de l'extension K/k (cf §1.3,c) du chapitre II).

On remarque que si k/F est ramifiée, $\frac{e'_0}{p-1}$ est impair car t doit être impair, nous utiliserons ce résultat dans b).

b) Nous allons prendre α dans F et $K = k(\alpha^{1/p})$. K/F est alors une extension galoisienne et diédrale, en effet : $\tau\alpha = \alpha$ et $\tau\zeta = \zeta^{-1}$.

Plus précisément :

- si k/F est non ramifiée on prend $\alpha = 1 + \lambda \varpi'^u$, où λ est une unité de F et où $u = \frac{pe'_0}{p-1} - t$. u est premier à p et $u < \frac{pe'_0}{p-1}$.

Le nombre de ramification de $K = k(\alpha^{1/p})/k$ est : $\frac{pe'_0}{p-1} - u$, c'est-à-dire le nombre t que l'on s'était donné dans b).

- si k/F est ramifiée, on prend $\alpha = 1 + \lambda \varpi'^u$ où λ est une

unité de F et où $u = \frac{pe'_0}{p-1} - t$. u est premier à p , $u < \frac{pe'_0}{p-1}$ et u est pair puisque $\frac{e'_0}{p-1}$ et t sont impairs lorsque k/F est ramifiée.

Le nombre de ramification de $K : k(\alpha^{1/p})/k$ est : $\frac{pe'_0}{p-1} - u$, c'est-à-dire le nombre t choisi dans b).

3. ETUDE D'UN A-MODULE $\mathfrak{A}_\theta$.

On pose pour tout i , $0 \leq i \leq p-1$:

$$e_i = g^i(1-\tau) \quad \text{et} \quad e'_i = g^i(1+\tau).$$

3.1. Propriétés relatives à l'élément g de $F[G]$.

Lemme 1.

Pour tout entier i , positif ou nul on a :

$$\tau \cdot g^i = (-1)^i g^i \cdot \tau.$$

Lemme 2.

Si $t \geq 1$ et si x est un élément de B on a, si p ne divise pas $v_K(x)$:

$$v_K(g \cdot x) = v_K(x) + t.$$

Démonstration :

Le lemme 1 est évident du fait que $\tau(\sigma^{-1}) = -(\sigma^{-1}) \cdot \tau$.

Le lemme 2 se démontre comme le lemme 1 du chapitre II en remarquant que :

$$g = \sigma^{-1}(\sigma^2 - 1).$$

Lemme 3.

g est entier sur A , son polynôme minimal est :

$$X^p + pa_{p-2}X^{p-2} + pa_{p-4}X^{p-4} + \dots + pa_3X^3 + pa_1X = 0$$

où les a_i , $1 \leq i \leq p-2$, sont dans $\mathbb{Z}$ et où $a_1 \not\equiv 0 \pmod{p}$.

Démonstration :

$$g^p = (\sigma - \sigma^{-1})^p = p(\sigma^{p-2} - \sigma^2) + \binom{p}{2}(\sigma^{p-4} - \sigma^4) + \dots \pm \frac{p}{2}(\sigma - \sigma^{-1}) .$$

On montre ensuite par récurrence que, pour $0 \leq i \leq \frac{p-3}{2}$, $\sigma^{2i+1} - \sigma^{-(2i+1)}$ est un polynôme en $\sigma - \sigma^{-1}$, à coefficients dans A , de degré $2i+1$, ne contenant que des puissances impaires de $\sigma - \sigma^{-1}$; et que de plus le coefficient de $(\sigma - \sigma^{-1})$ dans ce polynôme est $2i+1$.

En effet $\sigma^{2i+1} - \sigma^{-(2i+1)} = (\sigma^{2i-1} - \sigma^{-(2i-1)})(\sigma^2 + \sigma^{-2}) - (\sigma^{2i-3} - \sigma^{-(2i-3)})$ et $(\sigma^2 + \sigma^{-2}) = (\sigma - \sigma^{-1})^2 + 2$. En faisant $i = \frac{p-1}{2}$ on trouve que $(\sigma - \sigma^{-1})^p = b'_{p-2}(\sigma - \sigma^{-1})^{p-2} + b'_{p-4}(\sigma - \sigma^{-1})^{p-4} + \dots + b'_3(\sigma - \sigma^{-1})^3 - p(\sigma - \sigma^{-1})$ avec $b'_i \in \mathbb{Z}$ pour $3 \leq i \leq p-2$.

g^p est donc un polynôme en g , dont les coefficients sont, dans $\mathbb{Z}$, des multiples de p . Ce polynôme ne contient que des puissances impaires de $(\sigma - \sigma^{-1})$; de plus le coefficient de $(\sigma - \sigma^{-1})$ s'écrit pa_1 où $a_1 \not\equiv 0 \pmod{p}$.

Lemme 4.

Si $1 \leq m \leq p-1$ on a

- pour m pair : $g^{p-1+m} = pb_{p-1}g^{p-1} + \dots + pb_m g^m + p^2 b_{m-2} g^{m-2} + \dots + p^2 b_2 g^2$.
 - pour m impair : $g^{p-1+m} = pb_{p-2} g^{p-2} + \dots + pb_m g^m + p^2 b_{m-2} g^{m-2} + \dots + p^2 b_1 g^1$.
- où les b_i sont des éléments de $\mathbb{Z}$ et où $b_m \not\equiv 0 \pmod{p}$.

Démonstration :

En multipliant l'égalité du lemme 3 :

$$g^p = -pa_{p-2}g^{p-2} - pa_{p-4}g^{p-4} - \dots - pa_1g$$

par les puissances successives de g ($g, g^2, g^3, \dots$) on obtient le lemme 4.

3.2. Détermination d'un A-module $\mathcal{U}_\theta$.

Dans le cas A :

En posant : $v_i = \left[\frac{it+a}{2p} \right]$, $v'_i = \left[\frac{it+a+p}{2p} \right]$ si a est impair

et $v_i = \left[\frac{it+a+p}{2p} \right]$, $v'_i = \left[\frac{it+a}{2p} \right]$ si a est pair

on obtient une base du A-module $\mathfrak{U}_\theta : \left(\frac{e_i}{\overline{v}_i}, \frac{e'_i}{\overline{v}'_i} \right)_{0 \leq i \leq p-1}$.

b) Si $a = 0$. D'après le paragraphe 2.3 de ce chapitre, k contient les racines p -èmes de l'unité et il existe π telle que π soit de trace nulle et que $\pi^p = \overline{\pi}$ soit uniformisante de k . De plus $t = \frac{2pe_0}{p-1}$.

Désignons par 1_{χ_i} les p idempotents de l'algèbre $k[H]$ définis dans la démonstration de la proposition 1 du chapitre II.

Si $\theta = (1+\pi^p)(1+\pi+\dots+\pi^{p-1})$

$$(1+\tau) \cdot \theta = 2(1+\pi^2+\dots+\pi^{p-1}+\pi^{p+1}+\dots+\pi^{2p-2})$$

$$(1-\tau) \cdot \theta = 2(\pi+\pi^3+\dots+\pi^p+\dots+\pi^{2p-1})$$

alors :

$$1_{\chi_0} (1+\tau) \cdot \theta = 1$$

$$1_{\chi_0} (1-\tau) \cdot \theta = \pi^p$$

et pour $0 \leq i \leq \frac{p-1}{2}$:

$$(1_{\chi_i} + 1_{\chi_{p-i}})(1-(-1)^i \tau) \cdot \theta = \pi^{p-i} + \pi^{p+i}$$

$$(1_{\chi_i} + 1_{\chi_{p-i}})(1+(-1)^i \tau) \cdot \theta = \pi^i + \pi^{2p-i}$$

$$\pi^p(1_{\chi_i} - 1_{\chi_{p-i}})(1-(-1)^i \tau) \cdot \theta = \pi^{2p-i} + \pi^{2p-i}$$

$$\pi^p(1_{\chi_i} - 1_{\chi_{p-i}})(1+(-1)^i \tau) \cdot \theta = \pi^{2p-p-i} + \pi^{p+i}$$

est une A-base de C , les $2p$ éléments décrits ci-dessus ayant des valuations toutes différentes et comprises de zéro à $2p-1$.

Pour $0 \leq i \leq \frac{p-1}{2}$, $(1_{\chi_i} + 1_{\chi_{p-i}})(1 \pm \tau)$, et $\pi^p(1_{\chi_i} - 1_{\chi_{p-i}})(1 \pm \tau)$ sont des éléments de $F[G]$. Par suite, $\mathfrak{U}_\theta$ est le sous A-module de $F[G]$ engendré par la famille :

$$(1_{\chi_0} (1+\epsilon \tau), (1_{\chi_i} + 1_{\chi_{p-i}})(1+\epsilon \tau) , \pi^p(1_{\chi_i} - 1_{\chi_{p-i}})(1+\epsilon \tau))$$

où i est un entier variant de 1 à $\frac{p-1}{2}$ et où ϵ est un entier prenant les valeurs 0 et 1.

On montre ensuite que $(\frac{e_i}{\bar{v}_i}, \frac{e'_i}{\bar{v}'_i})_{0 \leq i \leq p-1}$ où $v_i = v'_i = [\frac{it}{2p}] = [\frac{ie_0}{p-1}]$

et où $\bar{w} = \pi^{2p}$ est une autre base de A-module $\mathfrak{u}_\theta$.

En effet

$$\frac{g^i(1 \pm \tau)}{[\frac{ie_0}{p-1}]} = \sum_{j=1}^{p-1} \frac{(\zeta^j - \zeta^{-j})^i}{[\frac{ie_0}{p-1}]} (1\chi_j + (-1)^i 1\chi_{p-j})(1 \pm \tau) ,$$

- si i est pair $\frac{(\zeta^j - \zeta^{-j})^i}{[\frac{ie_0}{p-1}]}$ est une unité de A .

- si i est impair $\frac{(\zeta^j - \zeta^{-j})^{i-1}}{[\frac{(i-1)e_0}{p-1}]}$ est une unité de A et $\frac{\zeta^j - \zeta^{-j}}{[\frac{e_0}{p-1}]} = v\pi^p$

où v est une unité de A .

La matrice qui fait passer de la famille

$$(1\chi_0(1+\epsilon\tau), (1\chi_i + 1\chi_{p-i})(1+\epsilon\tau), \pi^p(1\chi_i - 1\chi_{p-i})(1+\epsilon\tau))_{1 \leq i \leq \frac{p-1}{2}}_{0 \leq \epsilon \leq 1}$$

à la famille $(\frac{e_i}{\bar{v}_i}, \frac{e'_i}{\bar{v}'_i})_{0 \leq i \leq p-1}$ a donc pour coefficients des unités de A et on démontre que son déterminant est une unité de A .

Dans le cas B :

Proposition 1 (B) :

Si $t \geq 1$, soit θ défini par :

- a) $\theta = u\pi^a$ si $a \neq 0$
- b) $\theta = u(1+\pi+\dots+\pi^{p-1})$ si $a = 0$.

Alors θ engendre une base normale de K/F et $\mathfrak{u}_\theta$ est le sous A-module

de $F[G]$ engendré par la famille : $(\frac{e_i}{\bar{v}_i}, \frac{e'_i}{\bar{v}'_i})_{0 \leq i \leq p-1}$ où :

$$v_i = [\frac{it+a}{p}] .$$

Démonstration de la proposition 1(B) :

a) Si $a \neq 0$. Si $v_i = \left[\frac{it+a}{p} \right]$ pour $0 \leq i \leq p-1$ la famille :

$$\left(\frac{g^i \cdot \pi^a}{v_i} \right)_{0 \leq i \leq p-1}$$
 est une B-base de C , en effet c'est une famille de p éléments de valuations toutes différentes (lemme 2) et comprises entre zéro et $p-1$.

$(u, \tau u)$ étant une base du A-module B , $(u - \tau u, u + \tau u)$ est une autre base de ce A-module et par suite puisque dans ce cas $\tau \pi = \pi$,

$$\left(\frac{g^i(1-\tau) \cdot u \pi^a}{v_i}, \frac{g^i(1+\tau) \cdot u \pi^a}{v_i} \right)_{0 \leq i \leq p-1}$$

est une A-base de C .

$\mathfrak{U}_\theta$ est alors le sous A-module de $F[G]$ engendré par la famille :

$$\left(\frac{e_i}{v_i}, \frac{e'_i}{v_i} \right)_{0 \leq i \leq p-1}$$
 .

b) Si $a = 0$. k contient les racines p -èmes de l'unité et on choisit l'uniformisante π telle que $\tau \pi = \pi$. Dans ce cas, $t = \frac{pe_0}{p-1}$ et $\pi^{2p} = \overline{\pi}$ est une uniformisante de F . D'après l'étude du cas cyclique (chapitre II), σ^2 jouant le même rôle que σ , on peut dire que la famille $\left(\frac{(\sigma^2 - 1)^i \cdot (1 + \pi + \dots + \pi^{p-1})}{v_i} \right)_{0 \leq i \leq p-1}$ est une B-base de C . Par suite, si l'on pose $v_i = \left[\frac{it}{p} \right] = \frac{ie_0}{p-1}$, la famille :

$$\left(\frac{(\sigma - \sigma^{-1})^i \cdot (1 + \pi + \dots + \pi^{p-1})}{v_i} \right)_{0 \leq i \leq p-1}$$
 est aussi une B base de C , en effet :

$$(\sigma - \sigma^{-1})^i = \sigma^{-i} (\sigma^2 - 1)^i \text{ pour } 0 \leq i \leq p-1 .$$

$(u - \tau u, u + \tau u)$ étant une base du A-module B , fixe par $g = \sigma - \sigma^{-1}$, on obtient une base du A-module C :

$$\left(\frac{g^i(1-\tau) \cdot \theta}{v_i}, \frac{g^i(1+\tau) \cdot \theta}{v_i} \right)_{0 \leq i \leq p-1} \text{ où } \theta = u(1 + \pi + \dots + \pi^{p-1}) .$$

$\mathfrak{U}_\theta$ est donc le sous-A-module de $F[G]$ engendré par la famille :

$$\left(\frac{e_i}{v_i}, \frac{e'_i}{v_i} \right)_{0 \leq i \leq p-1} \text{ avec } v_i = \frac{ie_0}{p-1} .$$

4. ETUDE DE L'EGALITE $\mathfrak{U}_\theta = \mathfrak{D}$.

Lemme 5.

Si M est le sous A -module de $F[G]$ engendré par la famille :

$$\left(\frac{e_i}{v_i}, \frac{e_i}{v'_i} \right)_{0 \leq i \leq p-1} \quad \text{avec} \quad 0 = v_0 = v'_0, \quad 0 \leq v_1 \leq v_2 \leq \dots \leq v_{p-1} \leq e_0 \quad \text{et}$$

$0 \leq v'_1 \leq \dots \leq v'_{p-1} \leq e_0$, M est un sous-anneau si et seulement si, pour tout couple (i, j) d'entiers compris entre 1 et $p-1$ on a :

- (1) si $i+j \leq p-1$: $v_i + v_j \leq v_{i+j}$ pour i ou j pair
 $v_i + v'_j \leq v'_{i+j}$ pour j impair
 $v'_i + v_j \leq v_{i+j}$ pour j impair
 $v'_i + v'_j \leq v'_{i+j}$ pour i ou j pair.
- (2) si $i+j \geq p$: $v_i + v_j \leq e_0 + v_{i+j+1-p}$ pour i ou j pair
 $v_i + v'_j \leq e_0 + v'_{i+j+1-p}$ pour j impair
 $v'_i + v_j \leq e_0 + v_{i+j+1-p}$ pour j impair
 $v'_i + v'_j \leq e_0 + v'_{i+j+1-p}$ pour i ou j pair.

Démonstration :

En utilisant les lemmes 1, 3 et 4 du paragraphe 3.1 de ce chapitre on montre facilement que :

$$\text{si } i+j \leq p-1 : \quad e_i e_j = \begin{cases} 2e_{i+j} & \text{si } j \text{ est pair} \\ 0 & \text{si } j \text{ est impair} \end{cases}, \quad e_i e'_j = \begin{cases} 0 & \text{si } j \text{ pair} \\ 2e'_{i+j} & \text{si } j \text{ impair} \end{cases}.$$

$$e'_i e_j = \begin{cases} 0 & \text{si } j \text{ est pair} \\ 2e_{i+j} & \text{si } j \text{ est impair} \end{cases}, \quad e'_i e'_j = \begin{cases} 2e'_{i+j} & \text{si } j \text{ pair} \\ 0 & \text{si } j \text{ impair} \end{cases}.$$

si $i+j \geq p$ et si $m = i+j+1-p$:

$$e_i e_j = \begin{cases} p b_{p-1} e_{p-1} + \dots + p b_m e_m + p^2 b_{m-1} e_{m-1} + \dots + p^2 b_1 e_1 & \text{si } j \text{ est pair} \\ 0 & \text{si } j \text{ est impair.} \end{cases}$$

$$e_i e'_j = \begin{cases} 0 & \text{si } j \text{ est pair} \\ pb_{p-1} e'_{p-1} + \dots + pb_m e'_m + p^2 b_{m-1} e'_{m-1} + \dots + p^2 b_1 e'_1 & \text{si } j \text{ est impair} \end{cases}$$

$$e'_i e_j = \begin{cases} 0 & \text{si } j \text{ est pair} \\ pb_{p-1} e_{p-1} + \dots + pb_m e_m + p^2 b_{m-1} e_{m-1} + \dots + p^2 b_1 e_1 & \text{si } j \text{ est impair} \end{cases}$$

$$e'_i e'_j = \begin{cases} pb_{p-1} e'_{p-1} + \dots + pb_m e'_m + p^2 b_{m-1} e'_{m-1} + \dots + p^2 b_1 e'_1 & \text{si } j \text{ est pair} \\ 0 & \text{si } j \text{ est impair.} \end{cases}$$

où les b_i sont des entiers de $\mathbb{Z}$ avec $b_m \not\equiv 0 \pmod{p}$.

On en déduit aisément les conditions (1) et (2) du lemme 5.

Dans le cas $\mathbb{A}$.

Proposition 2($\mathbb{A}$).

Si θ est l'élément défini dans la proposition 1($\mathbb{A}$) on a : $\mathfrak{U}_\theta = \mathfrak{O}$ si et seulement si : $a = 0$, $a = 1$ ou $a = p-1$.

Démonstration de la proposition 2($\mathbb{A}$) :

D'après la proposition 2 du chapitre I : $\mathfrak{U}_\theta = \mathfrak{O}$, si et seulement si $\mathfrak{U}_\theta$ est un sous-anneau de $F[G]$.

On applique alors le lemme 5 au $\mathbb{A}$ -module $M = \mathfrak{U}_\theta$.

- si $a = 0$, on vérifie facilement que $\mathfrak{U}_\theta$ est un sous-anneau de $F[G]$;
- si $a \neq 0$, la proposition se déduit des deux lemmes suivants :

Lemme 6($\mathbb{A}$).

Si a est impair et si $M = \mathfrak{U}_\theta$, les conditions (2) sont toujours vérifiées et les conditions (1) sont vérifiées si et seulement si : $a = 1$.

Lemme 7(A) .

Si a est pair et si $M = \mathfrak{U}_0$, les conditions (2) sont toujours vérifiées
pour $a = p-1$, elles sont vérifiées pour a quelconque seulement si
 $t \leq \frac{2pe_0}{p-1} - 1$; les conditions (1) sont vérifiées si et seulement si : $a = p-1$.

Démonstration du lemme 6(A) :

$$a) \quad \underline{\text{si } i+j \geq p} : \quad v_i + v_j = \left[\frac{it+a}{2p} \right] + \left[\frac{jt+a}{2p} \right] \leq \left[\frac{(i+j+1-p)t+a+(p-1)t+a}{2p} \right]$$

$$v_i + v'_j = \left[\frac{it+a}{2p} \right] + \left[\frac{jt+a+p}{2p} \right] \leq \left[\frac{(i+j+1-p)t+a+p+(p-1)t+a}{2p} \right]$$

$$v'_i + v'_j = \left[\frac{it+a+p}{2p} \right] + \left[\frac{jt+a+p}{2p} \right] \leq \left[\frac{(i+j+1-p)t+a+p+(p-1)t+a+p}{2p} \right]$$

or $\frac{(p-1)t+a+p}{2p} = \frac{(p-1)a_0}{2} + \frac{a+1}{2} \leq e_0$ si a est impair, donc les conditions (2) sont vérifiées quel que soit la parité de j et de i .

$$b) \quad \underline{\text{si } i+j \leq p-1} . \text{ Si } a \neq 1 , \text{ écrivons } \frac{a}{p} = \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots}}} = [a_1 a_2 \dots a_n] ,$$

le développement de $\frac{a}{p}$ en fraction continue.

- si $a_1 > 1$, alors $a_1 = n$ avec $2 \leq n < \frac{p}{3}$ (car $a \geq 3$) , c'est-à-dire :

$$\frac{p}{n+1} \leq a < \frac{p}{n} .$$

Posons : $i = n$ et, si n est pair : $j = n-1$, si n est impair : $j = n-2$.
 Dans les deux cas, $i+j < p-1$ et j est impair.

D'autre part, $v'_i + v_j > v_{i+j}$; en effet $v'_i = \left[\frac{it+a+p}{2p} \right] = i \frac{a_0}{2} + \left[\frac{(i+1)a+p}{2p} \right] = i \frac{a_0}{2} + \left[\frac{(n+1)a+p}{2p} \right]$

$$v_j = \left[\frac{jt+a}{2p} \right] = j \frac{a_0}{2} + \left[\frac{na}{2p} \right] \quad \text{et} \quad v_{i+j} = (i+j) \frac{a_0}{2} + \left[\frac{2na}{2p} \right] , \text{ or on a : } \left[\frac{2na}{2p} \right] = \left[\frac{na}{p} \right] = 0$$

$$\text{et, } \left[\frac{(n+1)a+p}{2p} \right] \geq 1 .$$

- si $a_1 = 1$, alors $a_2 = n$, $2 \leq n < p-1$ (car $a < p-1$) c'est-à-dire :

$$\frac{np}{n+1} \leq a < \frac{(n+1)p}{n+2} .$$

Posons si n impair : $i = 1$ et $j = n$; j est donc impair et $i+j = n+1 \leq p-1$.

On démontre comme ci-dessus que : $v'_i + v_j > v_{i+j}$.

Posons si n est pair : $i = 1$ et $j = n$; j est pair et $i+j \leq p-1$.

On montre de la même façon que : $v'_i + v'_j > v'_{i+j}$.

Dans les deux cas, les conditions (1) ne sont pas vérifiées. On en déduit que si a est impair et différent de 1 , $\mathfrak{U}_\theta$ n'est pas un anneau. On vérifie facilement que pour $a = 1$, $\mathfrak{U}_\theta$ est un sous-anneau de $F[G]$.

Démonstration du lemme 7(A) :

a) Si $i+j \geq p$. Comme dans le lemme 6(A) on a :

$$v_i + v_j \leq \left[\frac{(i+j+1-p)t+a+p+(p-1)t+a+p}{2p} \right]$$

$$v'_i + v_j \leq \left[\frac{(i+j+1-p)t+a+p+(p-1)t+a}{2p} \right]$$

$$v'_i + v'_j \leq \left[\frac{(i+j+1-p)t+a+(p-1)t+a}{2p} \right]$$

$$\text{Or } \frac{(p-1)t+a+p}{2p} = \frac{(p-1)a_0}{2} + \frac{(a+1)}{2} ; \text{ si } t \leq \frac{2pe_0}{p-1} - 1 : \frac{(p-1)a_0}{2} + \frac{(a+1)}{2} < e_0 \text{ et}$$

par suite les conditions (2) sont vérifiées.

Pour t quelconque, on vérifie directement que si $a = p-1$, tout couple (i,j) satisfait aux conditions (2).

b) $i+j \leq p-1$.

$$\begin{aligned} \blacksquare \text{ si } \underline{a = p-1} : v_i &= \left[\frac{it+a+p}{2p} \right] = i(a_0 - 1) + \left[\frac{ip+(i+1)(p-1)+p}{2p} \right] \\ &= i(a_0 - 1) + i + \left[\frac{2p-i-1}{2p} \right] \end{aligned}$$

$$v_i = i(a_0 - 1) + i = v'_i .$$

On vérifie alors facilement que tout couple (i,j) satisfait aux conditions (1) .

■ si $a \neq p-1$, montrons qu'il existe un couple (i,j) qui ne satisfait pas aux conditions (1). Plus précisément, nous allons montrer qu'il existe :

- soit un couple (i, j) avec i ou j pair et $i+j \leq p-1$ tel que :

$$v_1 + v_j > v_{i+j}, \text{ c'est-à-dire : } [(i+1)\frac{a+p}{2p}] + [(j+1)\frac{a+p}{2p}] > [(i+j+1)\frac{a+p}{2p}] \text{ ou}$$

$$\text{encore } \frac{a+p}{2p} + \underbrace{(i+j+1)\frac{a+p}{2p}} > \underbrace{(i+1)\frac{a+p}{2p}} + \underbrace{(j+1)\frac{a+p}{2p}}. \quad (c)$$

- soit un couple (i, j) avec j impair et $i+j \leq p-1$ tel que : $v_1 + v'_j > v'_{i+j}$
c'est-à-dire : $[(i+1)\frac{a+p}{2p}] + [\frac{(j+1)(a+p)-p}{2p}] > [\frac{(i+j+1)(a+p)-p}{2p}]$ ou encore

$$\frac{a+p}{2p} + \underbrace{\frac{(i+j+1)(a+p)-p}{2p}} > \underbrace{(i+1)\frac{a+p}{2p}} + \underbrace{\frac{(j+1)(a+p)-p}{2p}} \quad (d)$$

Il existe un entier k , $1 \leq k \leq p-2$, et un seul tel que :

$$\underbrace{(k+1)\frac{a+p}{2p}} = \frac{2p-1}{2p} \text{ ou } \frac{p-1}{2p}.$$

1°) il existe k , $1 \leq k \leq p-2$ tel que $\underbrace{(k+1)\frac{a+p}{2p}} = \frac{2p-1}{2p}$. Alors k est pair et : $2 \leq k \leq p-3$.

a) s'il existe i pair, $1 < i < k$ tel que $\underbrace{(i+1)\frac{a+p}{2p}} < \frac{a+p}{2p}$, le couple $(i, k-i)$ vérifie l'inégalité (c) puisque pour tout j strictement plus petit que k :

$$\underbrace{(j+1)\frac{a+p}{2p}} < \underbrace{(k+1)\frac{a+p}{2p}} = \frac{2p-1}{2p}.$$

b) si pour tout i pair $1 < i < k$, on a $\underbrace{(i+1)\frac{a+p}{2p}} > \frac{a+p}{2p}$ alors :
 $(k+1)a = p-1$.

En effet, on a : $\underbrace{\frac{3(a+p)}{2p}} > \frac{a+p}{2p}$, on en déduit que : $3a < p$.

De manière analogue si : $3a < p$ et $\underbrace{\frac{5(a+p)}{2p}} > \frac{a+p}{2p}$ on a : $5a < p$ et en poursuivant on arrive à : $(k-1)a < p$. Comme a est différent de $p-1$:

$$\underbrace{(k+1)\frac{a+p}{2p}} > \frac{a+p}{2p} \text{ et par suite on obtient : } (k+1)a < p.$$

Puisque $(k+1)(a+p) = (k+1)a + p + kp$ et que k est pair c'est que $(k+1)a = p-1$.

Posons alors $i = k+2$ et $j = 1$.

On a : $i+j = k+3 < p$ en effet, k ne peut pas prendre la valeur $p-3$.

$$\underbrace{(j+1)\frac{a+p}{2p}} = \frac{2a}{2p} < \frac{a+p}{2p}$$

et

$$\underbrace{(i+1)\frac{a+p}{2p}} = \underbrace{(k+3)\frac{a+p}{2p}} = \frac{2p-1}{2p} + \frac{2a}{2p} - 1 = \frac{2a-1}{2p} < \frac{2p-1}{2p}.$$

Le couple (i, j) vérifie l'inégalité (c).

2°) Il existe k , $1 \leq k \leq p-2$ tel que $\underbrace{(k+1)\frac{a+p}{2p}} = \frac{p-1}{2p}$. Alors k est impair.

a) si $k \geq 3$ et s'il existe i pair, $1 < i < k$ tel que :

$$\underbrace{(i+1)\frac{a+p}{2p}} < \frac{a+p}{2p}.$$

Le couple (i, j) avec $j = k-i$ impair, vérifie l'inégalité (d).

$$\text{En effet : } \underbrace{\frac{(j+1)(a+p)-p}{2p}} < \underbrace{\frac{(k+1)(a+p)-p}{2p}} = \frac{2p-1}{2p}.$$

b) si $k = 1$ ou si $k \geq 3$ et que pour tout i pair :

$$\underbrace{(i+1)\frac{a+p}{2p}} > \frac{a+p}{2p},$$

alors,

$$\underbrace{(k+1)a} = p-1.$$

En effet, si $k = 1$, $a = \frac{p-1}{2}$.

Si $k \geq 3$ par un raisonnement analogue à celui du 1°) on montre que $ka < p$ et par suite que $(k+1)a = p-1$.

Posons alors $i = k+1$ et $j = 1$.

On a : $i+j = k+2 \leq p-2$ car k ne peut prendre la valeur $p-2$.

$$\underbrace{(j+1)\frac{a+p}{2p}} = \frac{2a}{2p} < \frac{a+p}{2p}$$

et

$$\underbrace{(i+1)\frac{a+p}{2p}} = \underbrace{(k+2)\frac{a+p}{2p}} = \underbrace{\frac{(k+1)(a+p)+a+p}{2p}} = \frac{a-1}{2p} < \frac{p-1}{2p} = \underbrace{(k+1)\frac{a+p}{2p}}.$$

Le couple (i, j) vérifie l'inégalité (c).

Dans le cas B.

Proposition 2(B).

Si θ est l'élément défini dans la proposition 1(B) on a : $\mathfrak{U}_\theta = \mathfrak{D}$, si et seulement si $a = 0$ ou a divise $p-1$.

Démonstration de la proposition 2(B) :

D'après la proposition 2 du chapitre I, $\mathfrak{U}_\theta = \mathfrak{D}$ si et seulement si $\mathfrak{U}_\theta$ est un sous-anneau de $F[G]$. On applique le lemme 5 au cas où $M = \mathfrak{U}_\theta$.

- si $a = 0$, $v_i = \frac{ie_0}{p-1}$ pour $0 \leq i \leq p-1$ et les conditions du lemme 5 sont vérifiées.

- si $a \neq 0$, $v'_i = v_i = \left[\frac{it+a}{p} \right]$ pour $0 \leq i \leq p-1$, les conditions du lemme 5 sont dans ce cas les conditions du lemme 2 du chapitre II, par suite, on sait (lemme 3 du chapitre II) que ces conditions sont vérifiées si et seulement si a divise $p-1$.

5. DETERMINATION DE L'ORDRE ASSOCIE $\mathfrak{D}$.

Proposition 3 (cas $\mathbb{A}$ et $\mathbb{B}$).

On suppose que $t \geq 1$ et que de plus dans le cas $\mathbb{A}$ avec a pair :
 $1 \leq t \leq \frac{2pe}{p-1} - 1$. L'ordre associé $\mathfrak{D}$ à C est le sous A -module de $F[G]$
engendré par la famille : $\left(\frac{e_i}{\mathfrak{w} n_i}, \frac{e'_i}{\mathfrak{w} n'_i} \right)_{0 \leq i \leq p-1}$ où les entiers n_i et n'_i
sont donnés par :

$$n_i = \min \left\{ \min_{\substack{j \text{ pair} \\ 0 \leq j \leq p-1-i}} (v_{i+j} - v_j), \min_{\substack{j \text{ impair} \\ 1 \leq j \leq p-1-i}} (v'_{i+j} - v'_j) \right\}$$

$$n'_i = \min \left\{ \min_{\substack{j \text{ impair} \\ 1 \leq j \leq p-1-i}} (v_{i+j} - v_j), \min_{\substack{j \text{ pair} \\ 0 \leq j \leq p-1-i}} (v'_{i+j} - v'_j) \right\}.$$

Démonstration de la proposition 3 :

Soit $\mathfrak{D}'$ le sous A -module de $F[G]$ engendré par la famille :
 $\left(\frac{e_i}{\mathfrak{w} n_i}, \frac{e'_i}{\mathfrak{w} n'_i} \right)_{0 \leq i \leq p-1}$, où les entiers n_i et n'_i sont, pour $0 \leq i \leq p-1$, les plus grands entiers vérifiant :

$$\frac{e_i}{\mathfrak{w} n_i} \mathfrak{U}_\theta \subset \mathfrak{U}_\theta \quad \text{et} \quad \frac{e'_i}{\mathfrak{w} n'_i} \mathfrak{U}_\theta \subset \mathfrak{U}_\theta.$$

D'après la proposition 1 du chapitre I, on a : $\mathfrak{D}' \subset \mathfrak{D}$.

Nous allons tout d'abord déterminer les entiers n_i et n'_i ($0 \leq i \leq p-1$) puis montrer que $\mathfrak{D} = \mathfrak{D}'$.

a) Les relations utilisées pour démontrer le lemme 5 du paragraphe 4 de ce chapitre nous montrent que n_i et n'_i ($0 \leq i \leq p-1$) sont les plus grands entiers vérifiant les relations :

$$(1') \quad \text{si } i+j \leq p-1 : \begin{aligned} n_i + v_j &\leq v_{i+j} && \text{pour } j \text{ pair} \\ n_i + v'_j &\leq v'_{i+j} && \text{pour } j \text{ impair} \\ n'_i + v_j &\leq v_{i+j} && \text{pour } j \text{ impair} \\ \text{et } n'_i + v'_j &\leq v'_{i+j} && \text{pour } j \text{ pair.} \end{aligned}$$

$$(2') \quad \text{si } i+j \geq p : \begin{aligned} n_i + v_j &\leq e_o + v_{i+j+1-p} && \text{pour } j \text{ pair} \\ n_i + v'_j &\leq e_o + v'_{i+j+1-p} && \text{pour } j \text{ impair} \\ n'_i + v_j &\leq e_o + v_{i+j+1-p} && \text{pour } j \text{ impair} \\ \text{et } n'_i + v'_j &\leq e_o + v'_{i+j+1-p} && \text{pour } j \text{ pair.} \end{aligned}$$

Dans les conditions de la proposition 3, les relations (2') sont toujours vérifiées. En effet, on a $n_i \leq v_i$ et $n'_i \leq v'_i$ pour tout i , $0 \leq i \leq p-1$, d'après les relations (1'), et, les relations (2) du lemme 5 sont toujours satisfaites.

Des conditions (1') on déduit facilement les formules de la proposition 3 donnant les entiers n_i et n'_i .

Remarquons que pour tout i , $1 \leq i \leq p-1$, on a :

$$v_i - 1 \leq n_i \leq v_i.$$

En effet, l'entier $v_i - 1$ satisfait aux conditions (1') imposés à n_i et de même pour $1 \leq i \leq p-1$:

$$v'_i - 1 \leq n'_i \leq v'_i.$$

De plus $n_o = n'_o = 0$, $n_{p-1} = v_{p-1}$ et $n'_{p-1} = v'_{p-1}$.

b) Montrons que : $\mathfrak{D} \subset \mathfrak{D}'$.

Soit $\alpha = \sum_{i=0}^{p-1} a_i \frac{e_i}{w} + \sum_{i=0}^{p-1} b_i \frac{e'_i}{w}$ un élément de $\mathfrak{D}$, les coefficients a_i et b_i sont dans F .

D'après la remarque précédente on voit que pour tout i , $1 \leq i \leq p-1$, wa_i et wb_i sont dans A et que de plus a_o , b_o , a_{p-1} et b_{p-1} sont dans A .

■ Supposons que certains coefficients a_i de α ne soient pas dans A . Soit i_o le plus grand entier, $1 \leq i_o \leq p-2$, tel que a_{i_o} n'appartienne pas

à A . $\alpha' = \sum_{i=0}^{i_0} a_i \frac{e_i}{w_i} + \sum_{i=0}^{p-1} b_i \frac{e'_i}{w'_i}$ est encore dans $\mathfrak{D}$. De plus $n_{i_0} = v_{i_0} - 1$. Il existe donc :

- soit un j_0 pair tel que $i_0 + j_0 \leq p-1$ et $n_{i_0} + v_{j_0} = v_{i_0+j_0}$;
- soit un k_0 impair tel que $i_0 + k_0 \leq p-1$ et $n_{i_0} + v'_{k_0} = v'_{i_0+k_0}$.

Dans le premier cas, écrivons que : $\alpha' \frac{e_{j_0}}{w_{j_0}}$ est dans $\mathfrak{U}_\theta$ (proposition 1,

chapitre I) , $\alpha' \frac{e_{j_0}}{w_{j_0}} = \sum_{i=0}^{i_0-1} a_i \frac{2e_{i+j_0}}{w_{i+j_0}} + a_{i_0} \frac{2e_{i_0+j_0}}{w_{i_0+j_0}}$. On en déduit que a_{i_0} est dans A .

Dans le deuxième cas, écrivons que : $\alpha' \frac{e'_{k_0}}{w'_{k_0}}$ est dans $\mathfrak{U}_\theta$.

$\alpha' \frac{e'_{k_0}}{w'_{k_0}} = \sum_{i=0}^{i_0-1} a_i \frac{2e'_{i+k_0}}{w'_{i+k_0}} + a_{i_0} \frac{2e'_{i_0+k_0}}{w'_{i_0+k_0}}$. On en déduit aussi que a_{i_0} est dans A .

Il y a donc dans les deux cas contradiction avec l'hypothèse, on en déduit que pour tout i , $0 \leq i \leq p-1$, les a_i sont dans A .

■ Soit i_0 le plus grand entier, $1 \leq i_0 \leq p-2$ tel que b_{i_0} n'appartien-

ne pas à A . $\alpha'' = \sum_{i=0}^{i_0} b_i \frac{e'_i}{w'_i}$ est encore un élément de $\mathfrak{D}$. De plus

$n'_{i_0} = v'_{i_0} - 1$. Il existe donc : soit un j_0 impair tel que $n'_{i_0} + v_{j_0} = v_{i_0+j_0}$
soit un k_0 pair tel que $n'_{i_0} + v'_{k_0} = v'_{i_0+k_0}$.

Un raisonnement analogue au précédent prouve que dans les deux cas b_{i_0} est dans A . Par suite, pour tout i , $0 \leq i \leq p-1$, b_i est dans A , et α est un élément de $\mathfrak{D}'$.

Remarque 1(A). Dans le cas A avec a pair et si $t > \frac{2pe_0}{p-1} - 1$, on obtient un résultat analogue pour l'ordre associé $\mathfrak{D}$, mais les formules donnant les entiers

n_i et n'_i sont différentes. En effet, dans ce cas là, les relations (2) du lemme 5 n'étant pas toujours vérifiées, les relations (2') (démonstration de la proposition 3) ne le sont pas non plus. Aussi dans les formules donnant les entiers n_i et n'_i , interviennent les indices j tels que $i+j \geq p$.

Remarque 1(B). Dans le cas B, on a $v_i = v'_i = [\frac{i+a}{p}]$, aussi les formules donnant les entiers n_i et n'_i sont simplifiées et on obtient pour $0 \leq i \leq p-1$:

$$n_i = n'_i = \min_{0 \leq j \leq p-1} (v_{i+j} - v_j).$$

Limitée au cas B, la démonstration de la proposition 3 est donc aussi simplifiée.

Remarque 2.

- Dans le cas A, avec a impair on a:

$$v'_{p-1} = v_{p-1} + 1 = n'_{p-1} = n_{p-1} + 1 = \frac{(p-1)a}{2} + \frac{a+1}{2}.$$

- Dans le cas A, avec a pair on a:

$$v'_{p-1} = v_{p-1} = n'_{p-1} = n_{p-1} = \frac{(p-1)a}{2} + \frac{a}{2}.$$

- Dans le cas B, on a:

$$v'_{p-1} = v_{p-1} = n'_{p-1} = n_{p-1} = (p-1)a + a.$$

Cherchons à quelles conditions l'élément, $\frac{1}{p} \sum_{i=0}^{p-1} \sigma^{i(1+\tau)}$ de $F[G]$

appartient à l'ordre associé $\mathfrak{D}$.

Si l'on pose $f = \sigma - 1$, on a:

$$1 + \sigma + \dots + \sigma^{p-1} = f^{p-1} + pf^{p-2} + \binom{p}{2}f^{p-3} + \dots + pf.$$

Donc, si $f' = \sigma^2 - 1$, on a:

$$\sum_{i=0}^{p-1} \sigma^i = 1 + \sigma^2 + \sigma^4 + \dots = f'^{p-1} + pf'^{p-2} + \binom{p}{2}f'^{p-3} + \dots + pf'.$$

Or, $\sigma - \sigma^{-1} = \sigma^{-1}(\sigma^2 - 1) = g$. Par suite:

$$\sigma \sum_{i=0}^{p-1} \sigma^i = \sum_{i=0}^{p-1} \sigma^i = g^{p-1} + p(a_{p-2}\sigma g^{p-2} + a_{p-3}\sigma^2 g^{p-3} + \dots + a_1\sigma^{p-2}g)$$

où les a_i sont dans $\mathbb{Z}$ et $\sum_{i=0}^{p-1} \sigma^i(1+\tau) = e'_{p-1} + p\lambda$ où λ est un élément de $F[G]$.

$\frac{1}{p} \sum_{i=0}^{p-1} \sigma^i(1+\tau)$ est donc dans $\mathfrak{D}$ si et seulement si $e_o \leq n'_{p-1}$.

On en déduit que $\frac{1}{p} \sum_{i=0}^{p-1} \sigma^i(1+\tau)$ est dans $\mathfrak{D}$ si et seulement si :

dans le cas A avec a impair : $\frac{2pe_o}{p-1} - 2 \leq t < \frac{2pe_o}{p-1}$;

dans le cas A avec a pair : $\frac{2pe_o}{p-1} - 1 \leq t \leq \frac{2pe_o}{p-1}$;

dans le cas B : $\frac{pe_o}{p-1} - 1 \leq t \leq \frac{pe_o}{p-1}$.

6. ETUDE DU $\mathfrak{D}$ -MODULE C .

6.1. Proposition 4.

On suppose que l'extension K/F vérifie les conditions suivantes :

dans le cas A : a est impair, différent de 1 et $1 \leq t < \frac{2pe_o}{p-1} - 2$;
ou a est pair, différent de 0 et de p-1 et $1 \leq t < \frac{2pe_o}{p-1} - 1$;

dans le cas B : a est non nul, a ne divise pas p-1 et $1 \leq t < \frac{pe_o}{p-1} - 1$.

Alors $\mathfrak{U}_\theta$ n'est pas un idéal à gauche principal de $\mathfrak{D}$.

Démonstration de la proposition 4 :

Soit α un élément de $\mathfrak{U}_\theta$, on considère l'application A-linéaire, de $\mathfrak{D}$ dans $\mathfrak{U}_\theta$ définie par : $\lambda \rightarrow \lambda\alpha$. On note $M(\alpha)$ la matrice associée à cette application dans les bases respectives $(\frac{e_i}{w_i}, \frac{e'_i}{w_i})_{0 \leq i \leq p-1}$ et $(\frac{e_i}{v_i}, \frac{e'_i}{v_i})_{0 \leq i \leq p-1}$ de $\mathfrak{D}$ et de $\mathfrak{U}_\theta$.

Les coefficients de $M(\alpha)$ sont dans A , on les désigne par μ_{ji} , j et i étant des entiers compris entre zéro et $2p-1$.

α est un générateur de l'idéal à gauche $\mathfrak{U}_\theta$ de $\mathfrak{D}$ si et seulement si le déterminant de $M(\alpha)$ est une unité de A .

Dans les conditions de la proposition 4, nous allons montrer que pour tout α de $\mathfrak{U}_\theta$, le déterminant de $M(\alpha)$ est congru à zéro modulo l'idéal ϖA de A et que par conséquent $\mathfrak{U}_\theta$ n'est pas un idéal à gauche principal de $\mathfrak{D}$.

Remarquons tout d'abord que si α est un générateur de l'idéal $\mathfrak{U}_\theta$, on peut supposer que α s'écrit : $\alpha = 1 + \sum_{i=1}^{p-1} a_i \frac{e_i}{\varpi^i} + \sum_{i=1}^{p-1} b_i \frac{e'_i}{\varpi^i}$, les a_i et b_i étant dans A , ou encore $\alpha = \frac{1}{2}(1-\tau) + \frac{1}{2}(1+\tau) + \sum_{i=1}^{p-1} a_i \frac{e_i}{\varpi^i} + \sum_{i=1}^{p-1} b_i \frac{e'_i}{\varpi^i}$.

En effet, si : $\mathfrak{U}_\theta = \mathfrak{D}\alpha$, (comme dans la démonstration de la proposition 4 du chapitre I), α est un élément inversible de $F[G]$ et son inverse est dans $\mathfrak{D}$. Soit $\overline{M(\alpha)}$ la matrice du corps résiduel $\overline{F} = A/\varpi A$ ayant pour coefficients les $\overline{\mu_{ji}}$, $0 \leq i, j < 2p-1$; $\overline{\mu}$ étant l'image dans $\overline{F}$ de l'élément μ de A . Ecrivons $\overline{M(\alpha)}$.

- Dans la première colonne de $M(\alpha)$: $\mu_{0,0} = 1$ et $\mu_{p,0} = 0$.
- De même, $\mu_{0,p} = 0$ et $\mu_{p,p} = 1$ dans la p -ème colonne.
- Soit i un entier fixé, $1 \leq i \leq p-1$.

$$\frac{e_i}{\varpi^i} \alpha = \frac{e_i}{\varpi^i} + \sum_{\substack{j=2 \\ j \text{ pair}}}^{p-1} 2a_j \frac{e_{i+j}}{\varpi^{i+j}} + \sum_{\substack{j=1 \\ j \text{ impair}}}^{p-2} 2b_j \frac{e'_{i+j}}{\varpi^{i+j}}$$

$$\frac{e_i}{\varpi^i} \alpha = \frac{e_i}{\varpi^i} + \sum_{\substack{j=2 \\ j \text{ pair}}}^{p-1-i} 2a_j \frac{e_{i+j}}{\varpi^{i+j}} + \sum_{\substack{j=1 \\ j \text{ impair}}}^{p-1-i} 2b_j \frac{e'_{i+j}}{\varpi^{i+j}} + \varpi \lambda, \lambda \text{ élément de } \mathfrak{U}_\theta.$$

En effet, si $j+i \geq p$ nous savons que $v_i + v_j \leq e_o + v_{i+j+1-p}$ (avec dans le cas A, a pair : $t \leq \frac{2pe_o}{p-1} - 1$). On peut de plus démontrer que :

dans le cas A avec a impair, si $1 \leq t < \frac{2pe_o}{p-1} - 2$: $\frac{(p-1)a_o}{2} + \frac{a+1}{2} < e_o$ (voir démonstration du lemme 6(A), chapitre III) et donc

$$v_i + v_j < e_o + v_{i+j+1-p}.$$

dans le cas A avec a pair, si $1 \leq t < \frac{2pe_0}{p-1} - 1 : \frac{(p-1)a_0}{2} + \frac{a+1}{2} < e_0$ (voir démonstration du lemme 7(A), chapitre III) et donc

$$v_i + v_j < e_0 + v_{i+j+1-p} ;$$

dans le cas B, si $1 \leq t < \frac{pe_0}{p-1} - 1 : (p-1)a_0 + a < e_0$ (voir démonstration du lemme 3 chapitre II) et donc

$$v_i + v_j < e_0 + v_{i+j+1-p} .$$

On a aussi

$$v_i + v'_j < e_0 + v_{i+j+1-p}$$

$$v'_i + v_j < e_0 + v_{i+j+1-p}$$

$$\text{et } v'_i + v'_j < e_0 + v_{i+j+1-p} .$$

Donc si l'on décompose $\frac{e_{i+j}}{n_{i+v_j}}$ ou $\frac{e'_{i+j}}{n'_{i+v'_j}}$, $i+j \geq p$, sur les $\frac{e_k}{v_k}$ et $\frac{e'_k}{v'_k}$, $0 \leq k \leq p-1$. Les coefficients sont nuls modulo ϖ .

On a donc :

$$\begin{cases} \overline{\mu_{j,i}} = 0 & \text{pour } 0 \leq j \leq i-1 \\ \overline{\mu_{i,i}} = 0 \text{ ou } 1 & \text{suivant que } n_i = v_i - 1 \text{ ou } n_i = v_i \\ \overline{\mu_{j,i}} = 0 & \text{pour } p \leq j \leq p+i . \end{cases}$$

■ Soit i , un entier fixé, $1 \leq i \leq p-1$, on a de même :

$$\frac{e'_i}{n'_i} \alpha = \frac{e'_i}{n'_i} + \sum_{\substack{j=1 \\ j \text{ impair}}}^{p-1-i} 2a_j \frac{e_{i+j}}{n_{i+v_j}} + \sum_{\substack{j=1 \\ j \text{ pair}}}^{p-1-i} 2b_j \frac{e'_{i+j}}{n'_{i+v'_j}} + \varpi \lambda' , \quad \lambda' \text{ dans } \mathfrak{u}_\theta ,$$

$$\text{c'est-à-dire : } \begin{cases} \overline{\mu_{j,p+i}} = 0 & \text{pour } 1 \leq j \leq i \\ \overline{\mu_{j,p+i}} = 0 & \text{pour } p \leq j \leq p+i-1 \\ \text{et } \overline{\mu_{p+i,p+i}} = 0 \text{ ou } 1 & \text{suivant que } n'_i = v'_i - 1 \text{ ou } n'_i = v'_i . \end{cases}$$

La matrice $\overline{M(\alpha)}$ est du type :

1	0	0	0	0	0	0	0	0	0	0	0	0	0
	0_{ou_1}	0	0	0	0	0		0	0	0	0	0	0
		0_{ou_1}	0	0	0	0			0	0	0	0	0
			0_{ou_1}	0	0	0				0	0	0	0
				0_{ou_1}	0	0					0	0	0
					0_{ou_1}	0						0	0
						1							0
0	0	0	0	0	0	0	1	0	0	0	0	0	0
	0	0	0	0	0	0		0_{ou_1}	0	0	0	0	0
		0	0	0	0	0			0_{ou_1}	0	0	0	0
			0	0	0	0				0_{ou_1}	0	0	0
				0	0	0					0_{ou_1}	0	0
					0	0						0_{ou_1}	0
						0							1

Les cases laissées blanches, sont les $\overline{\mu_{j,i}}$ susceptibles d'être non nuls. On a $\overline{\mu_{p-1,p-1}} = 1$ car $n_{p-1} = v_{p-1}$ et $\overline{\mu_{2p-1,2p-1}} = 1$ car $n'_{p-1} = v'_{p-1}$ (voir remarque 2 du paragraphe 5 de ce chapitre).

On montre que : $\det \overline{M(\alpha)} = \prod_{i=0}^{2p-1} \overline{\mu_{ii}}$.

Dans les conditions de la proposition 4, $\mathfrak{U}_\theta$ est différent de $\mathfrak{D}$ (proposition 2(A) et 2(B)), il existe donc un indice i , au moins, tel que $n_i = v_i - 1$ ou $n'_i = v'_i - 1$.

On en déduit que $\det \overline{M(\alpha)} = 0$ pour tout α , et, par suite $\mathfrak{U}_\theta$ n'est pas, dans les conditions de la proposition 4, un idéal à gauche principal de $\mathfrak{D}$.

6.2. On résume les résultats de ce chapitre par le théorème.

Théorème.

a) Si $t \equiv 0$ (modulo p) : C est un $\mathfrak{D}$ -module libre.

b) Si $t \not\equiv 0$ (modulo p) :

dans le cas A :

- si a est impair et si $t < \frac{2pe_o}{p-1} - 2$, C est un $\mathfrak{D}$ -module libre
si et seulement si : $a = 1$.

- si a est pair et si $t < \frac{2pe_o}{p-1} - 1$, C est un $\mathfrak{D}$ -module libre si
et seulement si : $a = p-1$.

dans le cas B :

- si $t < \frac{pe_o}{p-1} - 1$, C est un $\mathfrak{D}$ -module libre si et seulement si a
divise $p-1$.

Démonstration du théorème :

D'après la proposition 2(ii) du chapitre I et les propositions 2(A) et 2(B) de ce chapitre, C est un $\mathfrak{D}$ -module libre si :

dans le cas A : $a = 0$, $a = 1$ ou $a = p-1$.

dans le cas B : $a = 0$ ou a divise $p-1$.

D'après la proposition 2(iv) du chapitre I et la proposition 4 de ce chapitre, C n'est pas libre sur $\mathfrak{D}$ si :

dans le cas A : a impair différent de 1 et $1 \leq t < \frac{2pe_o}{p-1} - 2$;

dans le cas A : a pair différent de 0 et de $p-1$ et $1 \leq t < \frac{2pe_o}{p-1} - 1$;

dans le cas B : a différent de 0 , ne divisant pas $p-1$ et $1 \leq t < \frac{pe_o}{p-1} - 1$.

Exemple 1 :

a) si $p = 3$. C est, quelle que soit l'extension diédrale K/F de degré 6 , un $\mathfrak{D}$ -module libre. En effet a ne peut prendre que les valeurs 0 , 1 et $p-1 = 2$.

b) Supposons $p \geq 7$ et prenons $k = \mathbb{Q}_p(\zeta)$ (ζ racine p -ème de l'unité).

Soit $F = \mathbb{Q}_p(\zeta + \zeta^{-1})$; l'élément $\alpha = 1 + (\zeta - \zeta^{-1})^4$ est dans F et d'après le paragraphe 2.4 de ce chapitre $K = k(\alpha^{1/p})$ est une extension diédrale de F . Le nombre de ramification de K/k est : $a = t = p-4$ (cf. §2.4). Comme a est impair et que $1 < t < p-2$, C n'est pas un $\mathfrak{D}$ -module libre.

Remarque 3.

Si $F = \mathbb{Q}_p$, pour $p > 3$ on a toujours $t = 1$ (en effet $t \leq \frac{2p}{p-1}$), pour $p = 3$ on a $t = 1$ ou $t = 3$ (cf. [8] et [1]).

Dans le cas $F = \mathbb{Q}_p$, les propositions 2(A) et 2(B) nous montrent donc que C est libre sur $\mathfrak{D}$.

Cette remarque peut se déduire des résultats de [1] en utilisant la proposition 5 du chapitre I.

Corollaire.

Soit K/F une extension, diédrale de degré $2p$, de corps de nombres vérifiant les conditions du paragraphe 3 du chapitre I. On note t le plus grand nombre de ramification de l'extension $K_{\mathfrak{p}}/F_{\mathfrak{p}}$ et a le reste de t modulo p . Si $t \not\equiv 0 \pmod{p}$ et si :

dans le cas A, $t < \frac{2pe_0}{p-1} - 2$ et $a \neq 1$ si a est impair ;

$t < \frac{2pe_0}{p-1} - 1$ et $a \neq p-1$ si a est pair ;

dans le cas B, $t < \frac{pe_0}{p-1} - 1$ et a ne divise pas $p-1$.

Alors C n'est pas un $\mathfrak{D}$ -module libre.

Démonstration :

On déduit ce corollaire du théorème précédent à l'aide de la proposition 5 du chapitre I.

Exemple 2.

Soit $k = \mathbb{Q}(\zeta) = \mathbb{Q}^{(p)}$, ζ racine p -ème de l'unité avec $p \geq 7$ et soit F le sous-corps réel maximal de $\mathbb{Q}^{(p)}$. Posons $\alpha = 1 + (\zeta - \zeta^{-1})^4$, alors $K = k(\alpha^{1/p})$ est une extension diédrale de F (cf. §2.4 de ce chapitre).

Désignons par $\mathfrak{P}$ l'idéal de K au-dessus de p , en complétant par rapport à $\mathfrak{P}$ on retrouve la situation de l'exemple 1-b) et on en déduit (proposition 5 du chapitre I) que C n'est pas libre sur $\mathfrak{O}$.

6.3. La question que nous nous posions au début de ce chapitre était : "si K/F est une extension diédrale de degré $2p$ d'un corps local F , l'anneau C des entiers de K est-il ou non un $\mathfrak{O}$ -module libre ?".

Le théorème précédent permet de répondre à cette question pour toutes les extensions K/F , exceptées les extensions où :

dans le cas A : a est impair, différent de 1 et $t \geq \frac{2pe_o}{p-1} - 2$,

dans le cas A : a est pair, non nul, différent de $p-1$ et $t \geq \frac{2pe_o}{p-1} - 1$,

dans le cas B : a est non nul, ne divise pas $p-1$ et $t \geq \frac{pe_o}{p-1} - 1$.

Dans les cas ci-dessus le nombre de ramification t est tel que l'élément : $\frac{1}{p} \sum_{i=0}^{p-1} \sigma^i(1+\tau)$ de $F[G]$ appartienne à l'ordre associé $\mathfrak{O}$.

On remarque que le corps F étant donné, ces exceptions ne concernent qu'une ou deux valeurs possibles pour t .

Il est probable qu'en utilisant des méthodes analogues à celles employées pour la situation correspondante du cas cyclique de degré p (paragraphe 5 du chapitre II), ces cas restants pourront être résolus.

BIBLIOGRAPHIE

- [1] A.M. BERGE - "Sur l'arithmétique d'une extension diédrale".
Séminaire Delange-Pisot-Poitou, 1970-71, n° 14.
- [2] N. BOURBAKI - "Algèbre commutative". Chapitre II et chapitre IV.
Hermann 1961.
- [2 bis] N. BOURBAKI - "Algèbre". Chapitre III.
Hermann.
- [3] M. DEURING - "Algebren".
Springer Verlag 1935.
- [4] A. FROEHLICH - "The module structure of Kummer extensions over
Dedekind domains".
Jour. reine angew Math. t.209 (1962), pp. 39-53.
- [4 bis] H. HASSE - "Invariant Kennzeichnung..."
Abhandlungen der deutschen Akademie der Wissenschaften
zu Berlin t.8 (1947), pp. 1 à 56.
- [5] H. JACOBINSKI - "Über die Hauptordnung eines Körpers als Gruppenmodul".
Jour. reine angew Math. t.213 (1964).
- [6] H.W. LEOPOLDT - "Über die Hauptordnung der ganzen Elementen eines
abelschen Zahlkörper".
Jour. reine angew Math. t.201 (1959), pp. 119-149.
- [7] R.E. MACKENZIE - "Artin Schreier equations in characteristic zero".
et G. WHAPLES
American jour. Math. t.78 (1956), pp. 473-485.

- [8] J. MARTINET - "Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre $2p$ ".
Annales de l'Institut Fourier, 19, 1(1969), pp. 1-80.
- [9] J. MARTINET - "Anneau des entiers d'une extension galoisienne considéré comme module sur l'algèbre du groupe de Galois".
Colloque Th. Nombres (1969, Bordeaux), Bull. Soc. Math. France, Mémoire 25, 1971, pp. 123-126.
- [10] E. NOETHER - "Normal Basis bei Körpern ohne höhere Verzweigung".
Jour. reine angew Math. t.167 (1932), pp. 147-152.
- [11] J.J. PAYAN - Cours sur les extensions de Kummer. Grenoble 1969.
- [12] J.P. SERRE - "Corps locaux".
Hermann 1962.

LISTE DES PROFESSEURS

Président : Monsieur Michel SOUTIF
Vice Président : Monsieur Gabriel CAU

PROFESSEURS TITULAIRES.

MM. ANGLES D'AURIAC Paul	Mécanique des fluides
ARNAUD Georges	Clinique des maladies infectieuses
ARNAUD Paul	Chimie
AYANT Yves	Physique approfondie
Mme BARBIER Marie-Jeanne	Electrochimie
MM. BARBIER Jean-Claude	Physique expérimentale
BARBIER Reynold	Géologie appliquée
BARJON Robert	Physique nucléaire
BARNOUD Fernand	Biosynthèse de la cellulose
BARRA Jean-René	Statistiques
BARRIE Joseph	Clinique chirurgicale
BENOIT Jean	Radioélectricité
BESSON Jean	Electrochimie
BEZES Henri	Chirurgie générale
BLAMBERT Maurice	Mathématiques Pures
BOLLIET Louis	Informatique (IUT B)
BONNET Georges	Electrotechnique
BONNET Jean-Louis	Clinique ophtalmologique
BONNET-EYMARD Joseph	Pathologie médicale
BONNIER Etienne	Electrochimie Electrometallurgie
BOUCHERLE André	Chimie et Toxicologie
BOUCHEZ Robert	Physique nucléaire
BRAVARD Yves	Géographie
BRISSENEAU Pierre	Physique du solide
BUYLE-BODIN Maurice	Electronique
CABANAC Jean	Pathologie chirurgicale
CABANEL Guy	Clinique rhumatologique et hydrologie
CALAS François	Anatomie
CARRAZ Gilbert	Biologie animale et pharmacodynamie
CAU Gabriel	Médecine légale et Toxicologie
CAUQUIS Georges	Chimie organique
CHABAUTY Claude	Mathématiques Pures
CHARACHON Robert	Oto-Rhino-Laryngologie
CHATEAU Robert	Thérapeutique
CHENE Marcel	Chimie papetière
COEUR André	Pharmacie chimique
CONTAMIN Robert	Clinique gynécologique
COUDERC Pierre	Anatomie Pathologique
CRAYA Antoine	Mécanique
Mme DEBELMAS Anne-Marie	Matière médicale
MM. DEBELMAS Jacques	Géologie générale
DEGRANGE Charles	Zoologie
DESSAUX Georges	Physiologie animale
DODU Jacques	Mécanique appliquée
DREYFUS Bernard	Thermodynamique
DUCROS Pierre	Cristallographie
DUGOIS Pierre	Clinique de Dermatologie et Syphillographie
FAU René	Clinique neuro-psychiatrique
FELICI Noël	Electrostatique
GAGNAIRE Didier	Chimie physique
GALLISSOT François	Mathématiques Pures
GALVANI Octave	Mathématiques Pures
GASTINEL Noël	Analyse numérique
GERBER Robert	Mathématiques Pures
GIRAUD Pierre	Géologie
KLEIN Joseph	Mathématiques Pures
Mme KOFER Lucie	Botanique et Physiologie végétale
MM. KOSZUL Jean-Louis	Mathématiques Pures
KRAVTCHENKO Julien	Mécanique
KUNTZMANN Jean	Mathématiques appliquées
LACAZE Albert	Thermodynamique
LACHARME Jean	Biologie végétale
LATREILLE René	Chirurgie générale
IATURAZE Jean	Biochimie pharmaceutique
LAURENT Pierre	Mathématiques appliquées
LEDRU Jean	Clinique médicale B
LLIBOUTRY Louis	Géophysique
LOUP Jean	Géographie
Mlle LUTZ Elisabeth	Mathématiques Pures
MM. MALGRANGE Bernard	Mathématiques Pures
MALINAS Yves	Clinique obstétricale
MARTIN-NOEL Pierre	Seméiologie médicale
MASSEPORT Jean	Géographie
MAZARE Yves	Clinique médicale A
MICHEL Robert	Minéralogie et Pétrographie
MOURIQUAND Claude	Histologie
MOUSSA André	Chimie nucléaire
NEEL Louis	Physique du solide
OZENDA Paul	Botanique
PAUTHENET René	Electrotechnique
PAYAN Jean-Jacques	Mathématiques Pures
PEBAY-PEYROULA J.C.	Physique
PERRET René	Servomécanismes
PILLET Emile	Physique industrielle
RASSAT André	Chimie systématique

RENARD Michel	Thermodynamique
REULOS René	Physique industrielle
RINALDI Renaud	Physique
ROGET Jean	Clinique de pédiatrie et de puériculture
SANTON Lucien	Mécanique
SEIGNEURIN Raymond	Microbiologie et Hygiène
SENGEL Philippe	Zoologie
SILBERT Robert	Mécanique des fluides
SOUTIF Michel	Physique générale
TANCHE Maurice	Physiologie
TRAYNARD Philippe	Chimie générale
VAILLAND François	Zoologie
VAUQUOIS Bernard	Calcul électronique
Mme VERAIN Alice	Pharmacie galénique
M. VERAIN André	Physique
Mme VEYRET Germaine	Géographie
MM. VEYRET Paul	Géographie
VIGNAIS Pierre	Biochimie médicale
YOCOZ Jean	Physique nucléaire théorique

PROFESSEURS ASSOCIES

MM. BULLEMER Bernhard	Physique
RADHAKRISHNA Pidatala	Thermodynamique

PROFESSEURS SANS CHAIRE

MM. AUBERT Guy	Physique
BEAUDOING André	Pédiatrie
MM. BERTRANDIAS Jean Paul	Mathématiques appliquées
BIAREZ Jean Pierre	Mécanique
BONNETAIN Lucien	Chimie minérale
Mme BONNIER Jane	Chimie générale
MM. CARLIER Georges	Biologie végétale
COHEN Joseph	Electrotechnique
COUMES André	Radioélectricité
DEPASSEL Roger	Mécanique des fluides
DEPORTES Charles	Chimie minérale
DESRE Pierre	Métallurgie
DOLIQUE Jean-Michel	Physique des plasmas
GAUTHIER Yves	Sciences biologiques
GEINDRE Michel	Electroradiologie
GIDON Paul	Géologie et Minéralogie
GLENAT René	Chimie organique
HACQUES Gérard	Calcul numérique
JANIN Bernard	Géographie
Mme KAHANE Josette	Physique
MM. MULLER Jean-Michel	Thérapeutique
PERRIAUX Jean-Jacques	Géologie et minéralogie
POUJOUADOFF Michel	Electrotechnique
REBECQ Jacques	Biologie (CUS)
REVOL Michel	Urologie
REYMOND Jean-Charles	Chirurgie générale
ROBERT André	Chimie papetière
SARRAZIN Roger	Anatomie et chirurgie
SARROT-REYNAULD Jean	Géologie
SIBILLE Robert	Construction Mécanique
SIROT Louis	Chirurgie générale
Mme SOUTIF Jeanne	Physique générale
M. VALENTIN Jacques	Physique nucléaire

MAITRES DE CONFERENCES ET MAITRES DE CONFERENCES AGREGES

Mlle AGNIUS-DELOD Claudine	Physique pharmaceutique
ALARY Josette	Chimie analytique
MM. AMBLARD Pierre	Dermatologie
AMBROISE-THOMAS Pierre	Parasitologie
ARMAND Yves	Chimie
BEGUIN Claude	Chimie organique
BELORIZKY Elie	Physique
BENZAKEN Claude	Mathématiques appliquées
Mme BERTRANDIAS Françoise	Mathématiques pures
MM. BLIMAN Samuel	Electronique (E.I.E.)
BLOCH Daniel	Electrotechnique
Mme BOUCHE Liane	Mathématiques (C.U.S.)
MM. BOUCHET Yves	Anatomie
BOUSSARD Jean-Claude	Mathématiques appliquées
BOUVARD Maurice	Mécanique des fluides
BRIERE Georges	Physique expérimentale
BRODEAU François	Mathématiques (I.U.T. B)
BRUGEL Lucien	Energétique
BUISSON Roger	Physique
BUTEL Jean	Orthopédie
CHAMBAZ Edmond	Biochimie médicale
CHAMPETIER Jean	Anatomie et or gènesne
CHIAVERINA Jean	Biologie appliquée (E.F.P.)
CHIBON Pierre	Biologie animale

	COHEN-ADDAD J.P.	Spectrométrie physique
	COLOMB Maurice	Biochimie médicale
	CONTE René	Physique
	CROUZET Guy	Radiologie
	DURAND Francis	Métallurgie
	DUSSAUD René	Mathématiques (C.U.S.)
Mme	ETERRADOSSI Jacqueline	Physiologie
MM.	FAURE Jacques	Médecine légale
	GAVEND Michel	Pharmacologie
	GENSAC Pierre	Botanique
	GERMAIN Jean Pierre	Mécanique
	GIDON Maurice	Géologie
	GRIFFITHS Michaël	Mathématiques appliquées
	GROULADE Joseph	Biochimie médicale
	HOLLARD Daniel	Hématologie
	HUGONOT Robert	Hygiène et Médecine préventive
	IDELMAN Simon	Physiologie animale
	IVANES Marcel	Electricité
	JALBERT Pierre	Histologie
	JOLY Jean René	Mathématiques pures
	JOUBERT Jean Claude	Physique du solide
	JULLIEN Pierre	Mathématiques Pures
	KAHANE André	Physique générale
	KUHN Gérard	Physique
Mme	LAJZEROWICZ Jeannine	Physique
MM.	LAJZEROWICZ Joseph	Physique
	LANCIA Roland	Physique atomique
	LE JUNTER Noël	Electronique
	LEROY Philippe	Mathématiques
	LOISEAUX Jean Marie	Physique nucléaire
	LONGUEQUE Jean Pierre	Physique nucléaire
	LUU DUC Cuong	Chimie organique
	MACHE Régis	Physiologie végétale
	MAGNIN Robert	Hygiène et Médecine préventive
	MARECHAL Jean	Mécanique
	MARTIN-BOUYER Michel	Chimie (C.U.S.)
	MAYNARD Roger	Physique du solide
	MICOUD Max	Maladies infectieuses

	MOREAU René	Hydraulique (I.N.P.)
	NEGRE Robert	Mécanique
	PARAMELLE Bernard	Pneumologie
	PECCOUD François	Analyse (I.U.T. B)
	PEFFEN René	Métallurgie
	PELMONT Jean	Physiologie animale
	PERRET Jean	Neurologie
	PERRIN Louis	Pathologie expérimentale
	PFISTER Jean Claude	Physique du solide
	PHELIP Xavier	Rhumatologie
Mle	PIERY Yvette	Biologie animale
MM.	RACHAIL Michel	Médecine interne
	RACINET Claude	Gynécologie et obstétrique
	RICHARD Lucien	Botanique
Mme	RINAUDO Marguerite	Chimie macromoléculaire
MM.	ROMIER Guy	Mathématiques (I.U.T. B)
	ROUGEMONT (DE) J.	Neuro-Chirurgie
	STIEGLITZ Paul	Anesthésiologie
	STOEBNER Pierre	Anatomie pathologique
	VAN CUTSEM Bernard	Mathématiques appliquées
	VEILLON Gérard	Mathématiques appliquées (I.N.P.)
MM.	VIALON Pierre	Géologie
	VOOG Robert	Médecine interne
	VROUSSOS Constantin	Radiologie
	ZADWORNÝ François	Electronique

MAITRES DE CONFERENCES ASSOCIES

MM.	BOUDOURIS Georges	Radioélectricité
	CHEEKE John	Thermodynamique
	GOLDSCHMIDT Hubert	Mathématiques
	YACOUD Mahmoud	Médecine légale

CHARGES DE FONCTIONS DE MAITRES DE CONFERENCES

Mme	BERIEL Hélène	Physiologie
Mme	RENAUDET Jacqueline	Microbiologie

VU,

Grenoble, le

Le président de la thèse,

C. CHABAUTY

VU, et permis d'imprimer

Grenoble, le

Le président de l'Université
scientifique et médicale,

